BOOK OF ABSTRACTS

ISMS CONFERENCE 2026

MILITARY SCIENCES IN ACTION: FROM OPERATIONAL INSIGHTS TO DEFENCE INNOVATION



9-12 NOVEMBER
2026
TARTU, ESTONIA

BOOK OF ABSTRACTS

ISMS CONFERENCE 2026

MILITARY SCIENCES IN ACTION: FROM OPERATIONAL INSIGHTS TO DEFENCE INNOVATION

9-12 NOVEMBER 2026, TARTU

TABLE OF CONTENTS

FOREWORD 13
WORKING GROUP 1: WAR STUDIES 14
ISRAEL ALVES DE SOUZA JÚNIOR* CHILD SOLDIERS: FROM PARAGUAY WAR TO CYBERSPACE 15
JAHANGIR ARASLI* THE CASPIAN GATEWAYS: ASSESSING SECURITY THREATS, RISKS, AND CHALLENGES IN THE MARITIME DOMAIN 16
PETTERI BLOMVALL* POSTMODERN FIELD MANUAL - A TOOLBOX FOR FRAME-AWARENESS AND SITUATION-DEPENDENT TEMPO OF INNOVATION 17
POPA BRINDUSA* FROM HYBRID THREATS TO DEFENCE TRANSFORMATION: STRATEGIC COMMUNICATION AND SOCIETAL RESILIENCE IN CONTEMPORARY CONFLICT 18
ANDRE CARVALHO* OPERATIONAL ART IN THE AGE OF MACHINE REASONING 19
MIKE CRONIN* IMAGINARIES OF THE RUSSO-UKRAINIAN WAR: FOLK THEORIES, CONSPIRACY NARRATIVES, AND RUSSIAN DISINFORMATION AMONG US CONSERVATIVES 20
ŁUKASZ CUDNY* IS THE KALININGRAD REGION RUSSIA'S STRATEGIC SECURITY HUB? TECHNOLOGICAL CAPABILITIES, A2/AD STRATEGY, AND THE TRANSFORMATION OF BALTIC SECURITY 21
FABRIZIO DE LONGIS* THE NEW CYBER-AI COGNITIVE WARFARE 22
AHMED HASHIM* THE STRENGTHS AND WEAKNESSES OF THE IRANIAN PILLARS OF DETERRENCE (BAZDARANDEGI) AND DEFENSE (DEFA) 23
MIINA KAARKOSKI* CONCEPTUALIZING COGNITIVE WARFARE: MILITARY AND SOCIETAL IMPLICATIONS OF NATO'S APPROACH 24
PETER MEEDOM* THE UKRAINE WAR AND THE CRISIS OF RUSSIAN MILITARY THOUGHT 25
EDUARDO XAVIER FERREIRA GLASER MIGON* JARBAS ALFEU DE PAULA JUNIOR[2] QUANTUM TECHNOLOGIES AND THE TRANSFORMATION OF WARFARE: INFORMATION SUPERIORITY, STRATEGIC COMPETITION, AND THE FUTURE OF MILITARY POWER 26
OLENA PROKOPYSHYNA* HOW THE OFFENSIVE RUSSIAN MILITARY OPERATION AGAINST UKRAINE HAS CHANGED OSINT 27
RIKKE MICHELLE RIETVELD* BATTLEFIELD FORENSICS IN ACTION: FROM OPERATIONAL LESSONS TO AN INTEROPERABLE NATO CAPABILITY 28
ANDRE SIMONYI* YURIY NAPLYOKOV[2] STRATEGIC TURBULENCE AND THE FUTURE OF OPERATIONAL PLANNING IN CONTEMPORARY CONDITIONS 29
THOMAS SLENSVIK* ANDERS MCD SOOKERMANY[2] WHAT HAPPENS WHEN SYSTEMS ORIENTED DESIGN MEETS MILITARY PLANNING? METHODOLOGICAL OBSERVATIONS FROM FOUR PLANNING WORKSHOPS 30
MART SOONIK* MAI BEILMANN[2] THE DOMESTICATED FRONT LINE. CHILDREN'S WAR MEANING-MAKING AND COGNITIVE SECURITY IN A BORDERLAND STATE 31
FRISO STEVENS* ROOM FOR MANEUVER AFTER UKRAINE? TOWARD A TACTICAL DEFENSEORIENTED DOCTRINE FOR EUROPEAN NATO RESTORING SOME MOBILITY 32
ADAM SVENDSEN* THE VIRTUES OF INTELLIGENCE ENGINEERING (IE): HELPFUL AS A START FOR NAVIGATING UNCERTAINTY… 33
GONZALO VÁZQUEZ* THE GRAY ZONE OF SEA POWER IN THE 21ST CENTURY: IMPLICATIONS FOR NATO 34
STEPAN YAKYMIAK* ROBOTIZATION OF WAR: IRREVERSIBLE SHIFTS IN THE DEFENSE ECOSYSTEMS, MILITARY SCIENCE, AND EDUCATION 35

MARZENA ZAKOWSKA* BELOW THE THRESHOLD OF WAR: HYBRID PRESSURE AND CONTROLLED ESCALATION IN KOSOVO (2016–2026) 36
AGNIETE ZOTKEVICIUTE BANEVICIENE* TURNING WEAKNESS INTO DETERRENCE: THE LOGIC OF STRATEGIC EXPOSURE (PART I) 37
AGNIETE ZOTKEVICIUTE BANEVICIENE* STRATEGIC EXPOSURE AS A DETERRENCE-AMPLIFYING MECHANISM IN LITHUANIA'S NATO POSTURE (PART II) 38
WORKING GROUP 2: MILITARY HISTORY 39
GREGOR DE ROOY* HÉLIO FARIAS[2] FROM THE FIELD TO THE CURRICULA, A STUDY OF PERCEIVED THREAT AND INTELLECTUAL RESPONSES FROM BRAZILIAN GENERALS 40
JOSEPHINE DURANT* PASSING FOR LOCAL IN WWII OCCUPIED FRANCE: THE STRATEGIES OF F SECTION FEMALE SPIES 41
LENE EKHAUGEN* NORWEGIAN UN PEACEKEEPERS AND LEISURE IN GAZA: 'FOR BENEFIT AND ENJOYMENT' 42
MILENA ALICIA JAKSIC* FROM OPERATIONAL INTEGRATION TO MULTI-DOMAIN OPERATIONS: HISTORICAL LESSONS FROM LUFTWAFFE OPERATIONAL ART 43
THOMAS M. JAMISON* WAR STORIES: MILITARY FICTION AND PREPARATION FOR FUTURE WARS AS HISTORICAL CASES 44
PERIHAN KARADEMIR* OPERATIONAL ADAPTATION IN STEPPE WARFARE: FOUNDATIONS OF MONGOL MILITARY SUCCESS 45
JAKUB MAŁOLEPSZY* INTERWAR POLISH COUNTER-SABOTAGE EFFORTS AGAINST THE SOVIET UNION AS LESSONS FOR MODERN HYBRID THREATS ON NATO'S EASTERN FLANK 46
MICHAŁ MYDŁOWSKI* TECHNOLOGICAL INNOVATIONS AS A CHALLENGE FOR THE UNION AND CONFEDERATE ARMIES DURING THE AMERICAN CIVIL WAR 47
ETHAN RAFUSE* WARNINGS UNHEEDED: A TALE OF TWO OFFICERS AND USING THE PAST TO THINK ABOUT THE WARS OF THE FUTURE 48
VIESTURS RASNACIS* OPERATIONAL NECESSITY AND INSTITUTIONAL INNOVATION: THE LATVIAN BORDER GUARD IN DEFENCE TRANSFORMATION, 1991–1997 49
RAFAIL REKOUNIOTIS* THE RETURN OF TERRESTRIAL REALITY: LESSONS FROM INTERWAR GEOPOLITICAL CHOKEPOINTS 50
JEAN-PIERRE SCHERMAN* 'PEACEKEEPING OPERATIONS IN THE DRC ARE NOT PEACEFUL' THE SOUTH AFRICAN NATIONAL DEFENCE FORCE BATTLES AGAINST THE M-23 REBEL GROUP 51
EVANDRO SOARES* PEACE OPERATIONS AND THE HISTORICAL TRANSFORMATION OF INTELLIGENCE AFTER THE COLD WAR: ONUCI AND THE EVOLUTION OF MULTINATIONAL INFORMATION PRACTICES 52
JACOB THOMAS-LLEWELLYN* OLD HISTORY – NEW AUDIENCE: THE INFLUENCE OF THE MULBERRY HARBOURS ON CONTEMPORARY CHINESE PREFABRICATED INVASION PLATFORMS 53
JACOB THOMAS-LLEWELLYN* FUEL IN THE DEEP: THE PLANNING AND OPERATIONAL LESSONS OF PROJECT PLUTO, 1943-1945 54
TIAGO ABRÃO VILINGA* THE ROLE OF UN MISSIONS IN PEACEBUILDING IN ANGOLA (1989-1997) 55
ADRIAN WETTSTEIN* 'ALMOST ALL OF THE MEN ARE APATHETIC TO THE POINT THAT THEY COULD NOT CARE LESS WHETHER THEY ARE SHOT DEAD BY THEIR OWN OFFICERS OR BY THE RUSSIAN': THE GERMAN 'INFANTRY CRISIS' IN 1943/44. 56
WORKING GROUP 3: MILITARY TECHNOLOGY 57
OYKU CAGLAYAN* ALEKSANDRS STUPENKOVS[2], VIKTORS GUTAKOVSKIS[3], UGUR GOLAL[4] DEVELOPMENT OF A HIGH-EFFICIENT BATTERY PACK FOR THE UAV 58
ABDELLAH CHEHRI* PROTECTING DRONES: SMARTER SECURITY FOR A CONNECTED SKY 59

JARBAS ALFEU DE PAULA JUNIOR* EDUARDO XAVIER FERREIRA GLASER MIGON[2] QUANTUM SENSING, MILITARY EFFECTIVENESS, AND THE FUTURE TRANSPARENCY OF THE BATTLEFIELD 60
NATHAN ESKUE* THE CONVERGENCE OF EVOLVING THREATS, AI CAPABILITY, AND NEXT-GEN COMPUTING WILL CHANGE THE BATTLEFIELD 61
VIKTORS GUTAKOVSKIS* ARTIS IESMINS[2], MEHMET-EFE ILHAN[3] MODULAR STEEL PAYLOAD MUNITION FOR EUROPEAN FPV/UAV PLATFORMS 62
MIKE HARTNETT* TOM NUGENT[2] WIRELESS POWER BEAMING AND A NEW MARITIME DOMAIN AWARENESS CAPABILITY 63
TAL INBAR* THE ULTIMATE CHALLENGE: STRATEGIC, OPERATIONAL, AND TECHICAL LESSONS FROM IRAN'S MISSILE WARFARE 64
MD MUHIDUL ISLAM KHAN* INTELLIGENT SPECTRUM MANAGEMENT FOR DEFENCE: LEVERAGING AI-DRIVEN 6G COMMUNICATION ARCHITECTURES IN MULTI-DOMAIN MILITARY OPERATIONS 65
SUZANA LAMPREIA* VALTER VAIRINHOS[2], VICTOR LOBO[3] DYNAMIC MAINTENANCE ON SHIPS WITH PYTHON ... 66
MARCEL MANGOLD* SHIFTING SOCIO-TECHNICAL PARADIGM: THE CASE OF SWEDISH UAV CAPABILITY BUILD-UP 67
JUHA MATTILA* CYBER AND ELECTROMAGNETIC ACTIVITIES (CEMA) IN A MULTI-DOMAIN BATTLEFIELD 68
ANA MOITA* TOMAS CALAPEZ[2], PEDRO PONTES[3], JOAO TORRES[4] MICROCHANNEL BASED HEAT SINK FOR THE THERMAL MANAGEMENT IN UAVS: EFFECT OF TILT ANGLE UNDER STEADY STATE AND TRANSIENT CONDITIONS 69
VLAD ONEȚIU* FROM EARTHQUAKE ALERTS AND AI INTELLIGENCE TO MULTI-DOMAIN DEFENCE 70
JUUSO PELTTARI* TUOMAS JALONEN[2], EETU JÄRVI[3], JONI KENTALA[4], JARKKO MARIN[5], JAN MIETTINEN[6], JERE HEIKKINEN[7], TUOMAS MÄKINEN[8], HENRI LAMMINAHO[9] FROM ARMOR TO MIND: BALLISTIC PROTECTION AND COGNITIVE RESILIENCE AGAINST IEDS AND DRONE WARFARE 71
DANIELE SEGRETO* PRE-ENERGIZED LAUNCH ARCHITECTURES FOR ATTRITION-BASED COUNTERUAS DEFENCE SYSTEMS 72
GUNTIS SKUNSTINS* THE CHANGING FACE OF THE BALTIC DEFENSE INNOVATION ECOSYSTEM 73
ZI YANG* THE RUSSIA–UKRAINE WAR AND CHINA'S AI-DRIVEN MILITARY MODERNIZATION 74
KACPER ZDROJEWSKI* ARCHITECTING THE AUTONOMOUS BATTLEFIELD: SYNERGIZING AI DISTRIBUTED CONNECTIVITY, AND THE EVOLUTION OF HUMAN CONTROL 75
WORKING GROUP 4: LEADERSHIP, COMMAND-AND-CONTROL, AND BASIC COMPETENCIES 76
RAWAAH ALMAHASNEH* FROM VIRTUAL SIMULATION TO OPERATIONAL REALITY: INTEGRATING VR TECHNOLOGIES INTO CRISIS MANAGEMENT AND JOINT SECURITY TRAINING 77
BARIŞ ATEŞ* SELÇUK CANTÜRK[2] HEROIC COMMAND AND THE COSTS OF FRONTLINE LEADERSHIP: COMMAND CULTURE IN THE TURKISH MILITARY 78
JULIA BANAŚ* KNOWLEDGE TRANSFER IN CONTEMPORARY SECURITY GOVERNANCE: A DISCOURSE-DRIVEN ANALYSIS OF NATO, EU, AND UN RECOMMENDATIONS 79
ERIC BÉGIN* REIMAGINING CANADIAN NCM PROFESSIONAL MILITARY EDUCATION FOR 2035 80
ANDRÉ KORSMO BERNTSEN* RATIONALITY MOTIFS IN DECISION-MAKING THEORY AND PROFESSIONAL JUDGEMENT IN THE MILITARY 81
OLGA CHIRIAC* HUMAN ENCODING SCALE VERSUS ARTIFICIAL NEURAL NETWORKS: IMPLICATIONS FOR THE NATO COMMAND-AND-CONTROL ENTERPRISE 82
WILLIAM COMBES* COMMAND FIRST: AI IN THE HUMAN LOOP FOR COMPLEX OPERATIONAL ENVIRONMENTS83
DAVID GETSADZE* AGENTIC AI FOR TOTAL DEFENCE: TRANSLATING OPERATIONAL LESSONS FROM UKRAINE INTO RESILIENT COMMAND-AND-CONTROL FOR SMALL DEMOCRACIES 84

SWATI KARAL* ASHU PASRICHA[2], RUPANE GOYAT[3] FROM INSIGHTS TO INNOVATION: RETHINKING COMMAND, LEADERSHIP IN AI ASSISTED WARFARE 85
KHYATI SINGH* BRIDGING THE GAP – OPERATIONAL FEEDBACK AS THE ENGINE OF DEFENCE INNOVATION 86
CYRILL KISCHEL* THE IMPORTANCE OF THE HUMAN LAYER IN AN INCREASINGLY AUTOMATED OODA LOOP 87
RENATO KLOSS* FIT FOR PURPOSE: DOCTRINAL IMPLEMENTATION OF ROBOTIC AND AUTONOMOUS SYSTEMS FROM THE LESSONS OF UKRAINE AND GAZA 88
MICHELE MASTROENI* EMPOWERMENT FOR ADDRESSING COMPLEXITY IN THE ARMED FORCES: REFRAMING THE LEADERSHIP ANALOGY 89
KEVIN MATHERS* STRATEGIC MISSION COMMAND IN NATO: INFLUENCE, SENSING, AND THE HUMAN DIMENSION 90
NIKOLAOS MITROPOULOS* OPTICS OF MODERN CONFLICTS: HOW INFORMATION DISORDER LEADS TO DEFEAT AND PRACTICAL SOLUTIONS FOR LEADERS 91
JOHAN ÖSTERBERG* ANDREAS EDEVALD[2] THE JANUS FACE – A METAPHOR FOR INFORMATION INFLUENCE AND COGNITIVE BIASES 92
SOILI PAANANEN* MILITARY LEADERS AND COMPLEXITY - STRATEGIC LEVEL VIEWPOINT 93
PIER-AUDREY BONNIER * DAVID BÉLANGER[2] WOMEN IN LEADERSHIP ROLES IN THE CANADIAN ARMED FORCES 94
CEMIL SAĞLAM* FROM THE FIELD TO REFORM: THE PROFESSIONALIZATION EXPERIENCE OF THE TURKISH ARMED FORCES THROUGH SPECIALIST SERGEANTS 95
ROCCO PASCO SANTURRI III* FROM SEOUL TO THE SUWALKI GAP: A UNIFIED COMMAND BLUEPRINT FOR THE BALTICS 96
EVA SULA* THE INTEGRATION GAP: WHY OPERATIONAL LESSONS RARELY BECOME OPERATIONAL CAPABILITY 97
JANNE TÄHTINEN* KEY TENETS OF NATO'S ALLIED JOINT DOCTRINE AND MDO 98
KIRSTEN WILD* SARA RUSSO[2] COGNITIVE WARFARE, OODA LOOP, STRATEGY, AND DECISION-MAKING 99
WORKING GROUP 5: MILITARY LAW AND ETHICS 100
GABRIEL MATTHEW BERGMAN* SEMIOTIC SCAFFOLDING AND CHANGING VALUES: MILITARY PRAXIS IN THE AGE OF AUTOMATION. 101
SUMANTA BHATTACHARYA* BHAVNEET KAUR SACHDEV[2] ARTIFICIAL INTELLIGENCE-DRIVEN DEFENCE INNOVATION: TRANSFORMING OPERATIONAL DECISION-MAKING AND MULTI-DOMAIN MILITARY STRATEGY 102
JAN ASMUS BISCHOFF* LOST IN TRANSLATION? MILITARY CONCEPTS, DOCTRINE, AND THE CASE FOR COMPARATIVE MILITARY STUDIES 103
CAIO GRACO CAMPELO* TEMPORAL COMPRESSION OF DETERRENCE: RETHINKING STRATEGIC STABILITY IN THE AGE OF ARTIFICIAL INTELLIGENCE 104
SERAFIM CARVALHO* MARIA COSTEIRA[2] CRYPTOGRAPHIC VULNERABILITY AS HYBRID THREAT VECTOR: HOW POSTQUANTUM STANDARDISATION CHOICES SHAPE NATO'S EXPOSURE IN THE TRANSITION WINDOW 105
GITA LEITLANDE* DEFENDING IN AN UNJUST WORLD 106
ASTA MASKALIŪNAITĖ* MORAL SHIELD? LEGAL AND ETHICAL QUESTIONS OF TOTAL DEFENCE 107
IONELA-VALERIA POPESCU* DRAGOȘ-GEORGE IONICĂ[2] BETWEEN WAR AND PEACE: THE LEGAL ARCHITECTURE OF OFFENSIVE CYBER OPERATIONS UNDER INTERNATIONAL HUMANITARIAN LAW 108
AJSELA TOCI* NARRATIVES OF SOVEREIGNTY AND TERRITORIAL INTEGRITY: A COMPARATIVE DISCOURSE ANALYSIS OF THE WESTERN BALKANS AND GEORGIA THROUGH INTERNATIONAL LAW AND POLITICAL ETHICS EPOKA 109
LINA VIDAUSKYTĖ* A PHENOMENOLOGICAL ANALYSIS OF THE STRUCTURE OF DECISION MAKING IN AI SUPPORTED WARFARE 110

AULI VIIDALEPP* GABRIEL MATHEW BERGMAN[2] TOWARD AN ETHICAL DESIGN FRAMEWORK FOR AUTOMATED FUNCTIONS IN MILITARY SOCIOTECHNICAL SYSTEMS 111
ROUNDTABLES 112
JONAH BOYER* DAVID LAST[2] PASTORAL TO OPERATIONAL: THE ROLE OF CHAPLAINS IN BUILDING COHESION AND MORAL RESILIENCE IN DIVERSE FORCES 112
WORKING GROUP 6: SECURITY AND DEFENCE POLICY 113
TAHIR AZAD* HYPERSONIC WEAPONS AND THE TRANSFORMATION OF STRATEGIC STABILITY IN CONTEMPORARY WARFARE 114
SUMANTA BHATTACHARYA* BHAVNEET KAUR SACHDEV[2] THE MILITARIZATION OF CYBERSPACE, DIGITAL AUTHORITARIANISM, AND CROSS-BORDER DATA WARFARE: RECONCEIVING COOPERATIVE DEFENCE GOVERNANCE AND NATIONAL SECURITY IN THE ERA OF ALGORITHMIC CONFLICT 115
HAFEEZ BIN ROMAINOR* SOFT-HEDGING FOR RESILIENCE: MALAYSIA'S DEFENCE ACQUISITION IN THE AGE OF HYBRID AND MULTI-DOMAIN WARFARE 116
MARLENA BLICHARZ* ATTITUDES TOWARDS NUCLEAR WEAPONS AND NUCLEAR ENERGY AMONG YOUNG PEOPLE IN PL AND KOR. ABSTRACT PROPOSAL 117
JEIMY CANO* THE EVOLUTION OF STATE CYBER DEFENCES IN THE 21ST CENTURY: FROM ROBUST DEFENCES TO ANTIFRAGILE DEFENCES 118
ADEWUNMI JAMES FALODE* TERRORISM, BANDITRY, AND CRIMINALITY IN NIGERIA: A STRATEGIC ANALYSIS OF THE CRIME-TERROR NEXUS 119
FRANCESCO FIMIANI* DRONES, DETERRENCE, AND THE BALTIC GAP: THE STRATEGIC ADVANTAGE OF DOMESTIC DRONE PRODUCTION IN THE CASE OF ESTONIA 120
MARTA GĘBSKA* PERCEPTION OF THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES – RESULTS OF OWN RESEARCH IN THE US 121
CAROLA GRITELLA* FABIO BIONDI[2], GUERRINO MAZZAROLO[3] HYBRID ATTACKS AGAINST HEALTHCARE CRITICAL INFRASTRUCTURES (HCI): RESILIENCE AND DEFENSIVE OPERATIONS 122
OĞUZHAN GÜNGÖR* AYŞEGÜL BOSTAN[2] TÜRKIYE'S INDISPENSABLE STRATEGIC ROLE IN THE EUROPEAN SECURITY FRAMEWORK 123
SIDDHANT HIRA* BUILDING COGNITIVE RESILIENCE IN INDIA'S THREAT LANDSCAPE 124
MARTINS DA COSTA HUGO BRAS* CRISIS OF MULTILATERALISM, MODERN UN PEACEKEEPING OPERATIONS, AND BRAZIL'S STRATEGIC ROLE 125
MISAKO ISHIKAWA* THE GEOPOLITICS OF WORDS: RECOGNITION, DIPLOMATIC TRUST, AND CONFLICT RESOLUTION – LESSONS FROM YUGOSLAVIA (1990S TO THE EARLY 21ST CENTURY) 126
EMMANUEL KARAGIANNIS* DIVERGENT DEFENCE TRAJECTORIES: A COMPARATIVE ANALYSIS OF GREEK AND CYPRIOT MILITARY REFORMS 127
SUSAN KHAZAELI* FROM GRAY ZONE TO CONTINUOUS CONFLICT: RECONFIGURING DETERRENCE IN HYBRID WARFARE 128
KLEMEN KOCJANCIC* FROM TERRITORIAL DEFENCE TO TERRITORIAL FORCE: A TRANSFORMATION OF MILITARY STRATEGIC RESERVE FORCES IN SLOVENIA 129
IVANA KOVAČEVIĆ BEKIĆ* TATJANA ŠOLAJA[2] INFORMATION WARFARE AND NATIONAL SECURITY CHALLENGES OF SMALL STATES: STRATEGIC VULNERABILITIES AND RESILIENCE IN THE DIGITAL AGE 130
AGUSTIN MACIEL* JAPAN'S COUNTERSTRIKE CAPABILITY: PUSHING THE LIMITS OF A DEFENSE-ORIENTED POLICY 131
MAREKS MATISONS* THE CASE FOR HOMELAND OVER DOMESTIC: A LINGUISTIC AND CULTURAL ARGUMENT 132

NICOLE NEVES* THE REGIONALIZATION OF PEACE OPERATIONS AND THE RECONFIGURATION OF SECURITY GOVERNANCE IN AFRICA: A HISTORICAL-INSTITUTIONALIST FRAMEWORK 133
MILENA PALCZEWSKA* FROM CLIMATE CRISIS TO HUMAN MOBILITY: SECURITY IMPLICATIONS OF CLIMATE-INDUCED MIGRATION 134
DUMITRU-CATALIN VASILE* DIGITAL SOVEREIGNTY AND DEMOCRATIC LEGITIMACY IN AI-ENABLED DEFENCE GOVERNANCE 135
LUISA VAZ* GUSTAVO SIMÕES[2] AN ANALYSIS OF THE LITERATURE ON THE MILITARIZATION AND SECURITIZATION OF BRAZIL'S MIGRATION AGENDA 136
KATERINA VELJANOVSKA BLAZHEVSKA* GEOPOLITICAL TRANSFORMATIONS, STRATEGIC DELIBERATION AND DEFENCE ADAPTATION: REASSESSING STRATEGIC NORMS FOR CONTEMPORARY SECURITY CHALLENGES 137
WORKING GROUP 7: ARMED FORCES AND SOCIETY 138
EYAL BEN-ARI* MASS AND SOPHISTICATION: ISRAEL'S RESERVE FORCES AS A TEMPLATE FOR TWENTY-FIRST-CENTURY MILITARY INNOVATION 139
IEVA BĒRZIŅA* POLITICAL LITERACY TO COUNTER HYBRID THREATS: LESSONS FROM LATVIA 140
MORTEN BRAENDER* WALK THE TALK? THE ANTECEDENTS OF DEFENCE-WILLINGNESS IN DENMARK 141
CARLOS MICHEL CALLIRGOS* TRANS-INSTITUTIONALISATION AND THE DESIGN OF POST-SERVICE IDENTITY INFRASTRUCTURE: IMPLICATIONS FOR MILITARY FORCE SUSTAINABILITY 142
STEFANO DE ROSA* MILITARY SERVICE AND SOCIAL INTEGRATION: PEOPLE OF FOREIGN ORIGIN IN THE SWISS ARMED FORCES 143
GITANA DUDZEVIČIŪTĖ* THE RESILIENCE OF SMALL STATE SOCIETIES IN THE CONTEXT OF PERCEPTIONS OF SECURITY 144
OKSANA HUSS* ROLE OF LOCAL SELF-GOVERNMENTS IN BUILDING LAYERED RESILIENCE: LEARNING FROM UKRAINE 145
VYTAUTAS ISODA* THE INVESTMENT IN AND TRANSFORMATION OF PARAMILITARY ORGANIZATIONS IN THE BALTIC STATES SINCE THE RUSSIAN INVASION OF UKRAINE 146
AUSRA KAMINSKAITE* MEASURES TO RETAIN MILITARY PERSONNEL IN THE ARMED FORCES UNDER THE CURRENT SECURITY CONTEXT 147
KAIRI KASEARU* ELERI LILLEMÄE[2], LIINA-MAI TOODING[3] SOCIAL COHESION, MEDIA USAGE, AND PERCEPTION OF HYBRID THREATS WITHIN THE WHOLE-OF-SOCIETY APPROACH 148
MARO KETOLA* TEIJA SEDERHOLM[2] FINNISH VOLUNTARY NATIONAL DEFENCE AS A PILLAR OF TOTAL DEFENCE 149
ROBERTS KITS* CITIZEN ENGAGEMENT IN COUNTERING HYBRID THREATS: READINESS TO REPORT SUSPICIOUS ACTIVITIES IN THE BALTIC STATES 150
KRISTINA KIVISTIK* KAIRI KASEARU[2] SECURITIZATION IN ESTONIAN POLITICAL DISCOURSE: NON-CITIZENS' VOTING RIGHTS IN THE CONTEXT OF LOCAL GOVERNMENT COUNCIL ELECTIONS 151
MARCEL KOLB* CIVIL-MILITARY COOPERATION FOR MARITIME CRITICAL INFRASTRUCTURE PROTECTION: FROM AD HOC LIAISON TO INTEGRATED DEFENCE PREPAREDNESS 152
DAVID LAST* SURVIVING THE GREY ZONE: NATIONAL IDENTITY, COHESION, AND PROTECTING INSTITUTIONS. 153
JÚLIA LOPES* FROM LIBERAL PEACEBUILDING TO SOCIETAL RESILIENCE? (RE)INTERPRETING THE WOMEN, PEACE, AND SECURITY AGENDA IN CONTEMPORARY DEFENCE GOVERNANCE 154
LY LUKS* KAIRI KASEARU[2] FEMALE CONSCRIPTS' DROP-OUT RISK AND INTENTION TO JOIN EDF AS AN ACTIVE-DUTY MEMBER 155

MARIA MURUMAA-MENGEL* ANASTASIA ISABELLA POOLE[2], SIGRID AAS[3] INFLUENCER-STRATEGIES USED IN SECURITY POLITICS AND WAR: ANALYSING SOCIAL MEDIA COMMUNICATION OF POLITICAL/MILITARY ELITE ACTORS 156

NEERAJ* WHOLE-OF-SOCIETY DEFENCE IN A MULTIPOLAR ERA OF PERSISTENT HYBRID CONFLICTS: INDIA'S CIVIL-MILITARY INTEGRATION AS A MODEL FOR EU STRATEGIC AUTONOMY AND RESILIENCE 157

KHALID SHAFI* JENS MATHIESEN[2] MILITARY SUPPORT TO CIVIL AUTHORITIES AND SOCIETAL RESILIENCE: PAKISTAN'S EXPERIENCE OF COVID-19 AND CLIMATE-RELATED EMERGENCIES 158

KRISTJAN SILM* TIIA-TRIIN TRUUSA[2] MAKING DEFENSE PERSONAL: NARRATIVE PATHWAYS INTO VOLUNTARY DEFENSE IN ESTONIA 159

SILVIA SOMMARBERG* VESA VALTONEN[2], TEIJA SEDERHOLM[3] WATER SECURITY DURING CASCADING DISRUPTIONS: INSIGHTS FROM SCENARIO WORKSHOP IN FINLAND 160

RONEY SOUSA* JOINT AND INTERAGENCY GOVERNANCE IN HYBRID SECURITY ENVIRONMENTS: OPERATIONAL INSIGHTS FROM THE CATRIMANI OPERATION 161

STEPHEN TRYNOSKY* CLOSING THE GAP: A NEW CONCEPTION FOR NATO RESERVE COMPONENTS IN AN ERA OF GREAT POWER COMPETITION 162

DÁNIEL BERNÁT VAY* FUTURE OF THE MILITARY WORKFORCE IN NATO'S EASTERN FLANK: POLICY INNOVATION TO MITIGATE DEMOGRAPHIC CONSTRAINTS 163

AULI VIIDALEPP* SOCIOCULTURAL VULNERABILITIES EXPLOITED IN AI-ENABLED HYBRID INFLUENCE ACTIVITIES 164

DAĞHAN YET* ASYMMETRY OF COMFORT 165

WORKING GROUP 8: DEFENCE MANAGEMENT AND ECONOMICS 166

IMOH ANTAI* PRE-LOGISTICS DUE DILIGENCE IN DEFENCE AND MILITARY GROWTH: ABSORB, BLEND, OR COMBINE? 167

FATMA CENGİZ* EARLY WARNING FOR DISRUPTION RISK IN DEFENCE PROCUREMENT: FROM REACTIVE REGISTERS TO ANTICIPATORY SIGNALS 168

ANTONIO JOÃO DE OLIVEIRA VIANNA JUNIOR* GABRIELA ROCHA BERNARDES[2] STRATEGIC CAPABILITIES OF THE DEFENSE INDUSTRIAL BASE: A COMPARATIVE STUDY BETWEEN BRAZIL AND NATO COUNTRIES 169

ANTONIO JOÃO DE OLIVEIRA VIANNA JUNIOR* KARINA FURTADO RODRIGUES[2] A COMPARATIVE ANALYSIS OF DEFENSE INDUSTRIAL BASE INCENTIVE POLICIES: BRAZIL X LEADING EU NATIONS 170

VLAD DUMITRACHE* HOW DEFENSE ACQUISITION HAS EVOLVED IN A EUROPEAN CONTINENT WHERE RE-ARMING HAS BECOME A PRIORITY 171

HELIO CAETANO FARIAS* IN SEARCH OF STRATEGIC AUTONOMY: EUROPEAN DEFENCE INDUSTRIAL FINANCING MECHANISMS AND LESSONS FOR BRAZIL 172

JOÃO XAVIER GONÇALVES* FROM OPERATIONAL LESSONS TO FUNDED CAPABILITY: DEFENCE BUDGET ADMINISTRATION, RESOURCE ALLOCATION AND STRATEGIC READINESS IN PORTUGAL 173

GUSTAV GRANLUND* ACCELERATING DEFENCE INNOVATION IN SWEDEN: INSTITUTIONAL BARRIERS AND PATHWAYS FOR CIVIL-MILITARY-INDUSTRY COORDINATION 174

JAROSŁAW GRYZ* ENERGY CHAINS IN NATO'S MULTI-DOMAIN OPERATIONS 175

ROLAND HELLBERG* DAVID MANNING[2] LOGISTICAL SUPPORT REQUIREMENTS OF THE DISPERSED AIR BASE SYSTEM 176

NICK WALTER HEINRICH HUSMANN* CROSSING THE VALLEY OF DEATH: HOW RESOURCE ALLOCATION LOGICS SHAPE MILITARY INNOVATION SUCCESS UNDER CONDITIONS OF SCARCITY AND INSTITUTIONAL UNCERTAINTY 177

JĀNIS KONDRĀTS* JELENA PUNDURE[2], INGA JEKABSONE[3], ASTRA AUZIŅA-EMSIŅA[4], MARTINS VARGULIS[5] FROM DEFENCE INNOVATION TO ECONOMIC VALUE: AN EMPIRICAL ASSESSMENT METHOD FOR SMALL-STATE ECONOMIES 178

LINUS KÜHL* AN INDICATOR-BASED FRAMEWORK FOR ASSESSING HYBRID VULNERABILITIES IN ALLIED LOGISTICS SUPPLY CHAINS 179

RINGAILĖ KUOKŠTYTĖ* CAPACITY, NETWORK CAPITAL, OR CONVERGENCE? CENTRAL AND EASTERN EUROPEAN COUNTRIES IN THE EUROPEAN DEFENCE FUND (2022–2024) 180

YAN KWIZERA* THE ZIPLINE EFFECT: SOVEREIGN FRONTIER INFRASTRUCTURE AS A CATALYST FOR ACCELERATING MILITARY INNOVATION CYCLES 181

TIAGO MARQUES DOS SANTOS FILHO* OVERCOMING TECHNOLOGICAL DEPENDENCY IN SMALL UNMANNED AERIAL SYSTEMS (UAS): A TRIPLE HELIX MODEL FOR DUAL-USE MICRODRONES IN THE BRAZILIAN ARMY 182

MASHUDU MATHOHO* ASSESSING RENEWABLE ENERGY READINESS ON MILITARY BASES: A GEOSPATIAL ANALYSIS OF SOLAR ENERGY ADOPTION IN THE WEST COAST REGION OF SOUTH AFRICA 183

PETER PAPLER* INNOVATION-DRIVEN DEFENSE ORGANIZATIONS 184

ASHU PASRICHA* THE ECONOMICS OF PEACE IN EUROPE: A GAME-THEORETIC FRAMEWORK FOR CONFLICT PREVENTION AND DEFENCE INNOVATION 185

GALINA ŠEVČENKO-KOZLOVSKA* FISCAL AND ECONOMIC RISKS OF RAPIDLY GROWING DEFENCE EXPENDITURE: A STUDY OF PUBLIC FINANCE SYSTEM TRANSFORMATION 186

SALMA SHAHEEN* THE RISE OF INFORMALITY IN EDT GOVERNANCE: PRIVATE SECTOR DYNAMICS AND NUCLEAR-ARMED STATES 187

MARIO JOSE SIMOES MARQUES* BRIDGING OPERATIONAL INSIGHT AND DEFENCE INNOVATION: EU AND NATO RESEARCH PRIORITIES, SCIENTIFIC GAPS, AND OPPORTUNITIES IN CONTEMPORARY MILITARY TECHNOLOGY .. 188

LENA TRABUCCO* ALEXANDER HØGSBERG TETZLAFF[2] THE TRANSFERABILITY OF UKRAINIAN INNOVATION: A FOUR-LAYER FRAMEWORK FOR SMALL STATES 189

LOUISE TUMCHEWICS* SECURING THE UAV SUPPLY CHAIN 190

KRZYSZTOF WIATER* ADAM DUDA[2], MICHAŁ MARCINIAK[3] FROM CONTRACTING TO CAPABILITY: A STATUTORY ARCHITECTURE FOR "ARMAMENT AGENCY 2.0" AND THE REFORM OF DEFENCE ACQUISITION IN A SURGE-SPENDING ERA 191

WORKING GROUP 9: MILITARY EDUCATION 192

ISRAEL ALVES DE SOUZA JÚNIOR* MILITARY SCIENCES, BRAZILIAN EDUCATIONAL PROGRAMS, AND POTENTIAL PRIMARY OBJECTS OF STUDY 193

DAVID ATKINSON* THE SPACE TO THINK: JUDGEMENT CONDITIONING IN PROFESSIONAL MILITARY EDUCATION – DECISION-FORCING CASES FOR MISSION COMMAND UNDER COGNITIVE PRESSURE 194

FILIP BANÁŠ* TESTING WARGAME-BASED PREPARATION IN A LIVE MILITARY EXERCISE: EXPLORATORY EVIDENCE FROM A CONTROLLED FIELD EXPERIMENT 195

PARENTEAU DANIC* THE APOLITICAL STANCE OF OFFICERS IN AN ERA OF POLITICAL POLARIZATION: THE CENTRALITY OF CRITICAL THINKING IN THE EDUCATION OF OFFICER-CADETS 196

MATIAS FERREYRA WACHHOLTZ* RENE MOELKER[2] CULTURAL AWARENESS AND INTEROPERABILITY IN PEACE OPERATIONS 197

HANNA FORSBERG* ØRJAN ROGNE RISE[2] CULTIVATING HYBRID INTELLIGENCE: THE EDUCATIONAL IMPACT OF AI EXPLORATION IN MILITARY PLANNING 198

ALEKSANDAR GRIZHEV* VESNA POPOSKA[2], LJUPCO SOSOLOVSKI[3] FROM OPERATIONAL INSIGHT TO INSTITUTIONAL ADAPTATION: INTEGRATING HYBRID THREAT LESSONS INTO PROFESSIONAL MILITARY EDUCATION 199

ROBERT HILLIARD* DANIEL PACKHAM[2] ALTERNATE, ADAPTED, AND EMERGING: NEW EDUCATION AND TRAINING PATHWAYS TO OFFICERSHIP IN SWEDEN (AND UKRAINE). 200
PATRICK HOFSTETTER* MORE MILITARY. MORE ACADEMY: RESEARCH-BASED TALENT DEVELOPMENT IN PROFESSIONAL MILITARY EDUCATION 201
TAAVI LAANEPERE* TRAINING FOR LARGE-SCALE WAR AND MILITARY EFFECTIVENESS IN COMPARATIVE HISTORICAL PERSPECTIVE 202
ANDREW HOCK CHYE LIM* TECHNOLOGY ENABLED LEARNING TO DEVELOP STRATEGIC APPRECIATION: DESIGN, EXECUTION, AND ANALYTICAL FINDINGS IN EDUCATING MID-CAREER OFFICERS 203
ROBERT LUMMACK* UAS CAPABILITY DEVELOPMENT: TRENDS, REALITIES AND TRAINING NEEDS FOR IMPACTFUL ALLOCATION 204
HEMANT MALHOTRA* BEYOND THE TEXTBOOK: ADAPTING MILITARY EDUCATION FOR AI-ASSISTED HYBRID THREATS 205
RONALD MAÑEJE* INSTITUTIONALIZING STRATEGIC THINKING IN THE PHILIPPINE MILITARY ACADEMY THROUGH MIND SPORTS INTEGRATION 206
ISAAC MOFOKENG* ASSESSING THE RELATIONSHIP BETWEEN DIGITAL FINANCIAL LITERACY AND FINANCIAL WELL-BEING AMONG RECRUITS IN THE MILITARY SKILLS DEVELOPMENT SYSTEMS (MSDS) 207
NEERAJ* THINKING BEYOND THE BATTLEFIELD: OFFICER DEVELOPMENT IN THE AGE OF MULTI-DOMAIN OPERATIONS, HYBRID WARFARE, AND RAPID TECHNOLOGICAL CHANGE 208
AMER RIKOVIC* LEARNING HOW TO OPERATE TOGETHER 209
JILL SCOTT* CECILE MALARDIER-JUGROOT[2] RAPID RESPONSE IN SUPPORT OF NATIONAL SOVEREIGNTY: ACCELERATING RESEARCH AND INNOVATION FOR DEFENCE CAPABILITIES AT THE ROYAL MILITARY COLLEGE OF CANADA 210
KHALID SHAFI* JENS MATHIESEN[2] FROM THE ARCTIC TO THE THIRD POLE: CLIMATE SECURITY, STRATEGIC FORESIGHT, AND PROFESSIONAL MILITARY EDUCATION 211
ASKIN INCI SOKMEN ALACA* HUMAN–MACHINE TEAMING AND COGNITIVE AUGMENTATION IN FUTURE WARFARE: MILITARY IMPLICATIONS OF NEURAL INTERFACES AND IMMERSIVE TRAINING ENVIRONMENTS 212
ANDERS MCD SOOKERMANY* THOMAS SLENSVIK[2] FROM FRICTION TO TRACTION: DESIGNING EPISTEMIC SPACE FOR INNOVATION IN PROFESSIONAL MILITARY EDUCATION 213
ÜLLE SÄÄLIK* DEVELOPING MILITARY LEADERS: GROWTH, SHIFT, OR FLUCTUATION IN LEADERSHIP IDENTITY? 214
INGVILD TEGNANDER* NEGOTIATING PROFESSIONAL IDENTITY THROUGH FEEDBACK IN MILITARY LEADER EDUCATION IN NORWAY 215
RONALD TI* OPERATIONAL LOGISTICS: PME'S UGLY DUCKLING 216
JUVENCIO ANTONIO VASCONCELOS LOBO* MILITARY EDUCATION AND THE ENVIRONMENT: INSTITUTIONAL CONCEPTIONS IN THE BRAZILIAN ARMY (2014-2022) 217
SAMUEL ZILINCIK* FAITH KLIJIAN[2] COGNITIVE SUPERIORITY BEGINS WITH EMOTION SCIENCE LITERACY: THE CASE OF DOUBT 218
ROUNDTABLES 219
ANNE MARIE HAGEN* FRANCIS CLERMONT[2], KJETIL ENSTAD[3], ROLAND HELLBERG[4], OMHANI AMBRE NAIJA[5], DOROTA DOMALEWSKA[6], KATERINA VELJANOVSKA BLAZHEVSKA[7], PIOTR OKULSKI[8] CRITICAL THINKING IN PME: COMPETENCE, DISPOSITION, OR CAPABILITY? 219
WORKING GROUP 10: STRATEGY 221
ÖZGENUR AKTAN* THE DIALOGUE BETWEEN HEDGING AND NORDIC BALANCE IN SMALL STATE STRATEGY? 222
JĀNIS BĒRZIŅŠ* RUSSIA'S DRONE WAR IS NOT ABOUT DRONES 223

JUN YAN CHANG* ADRIAN U-JIN ANG[2] A FRIEND IN NEED IS A FRIEND INDEED: THE UNITED STATES AND ITS JOINT MILITARY EXERCISES IN THE ASIA-PACIFIC 224
EDMUND CURRY* STRATEGIC AGENCY UNDER DURESS: LESSONS FROM THE WINTER WAR FOR SMALL STATES 225
TERESA DE ALMEIDA E SILVA* DIOGO RIBEIRO CARDOSO[2] SPACE AS A DOMAIN OF SMALL-STATE AGENCY: PORTUGAL, THE AZORES, AND STRATEGIC RELEVANCE IN GREAT POWER COMPETITION 226
JEANETTE DE WEERT* SOCIETAL RESILIENCE AGAINST COGNITIVE WARFARE 227
DARRELL DRIVER* ARCTIC SECURITY REPORT: WHAT WE SHOULD WORRY ABOUT WHEN WE WORRY ABOUT THE ARCTIC 228
AMBER FRENCH-GRIETTE* THE CIVIC SHIELD: UNARMED RESISTANCE AS THE SECOND ARSENAL OF NATIONAL DEFENSE – LESSONS FROM UKRAINE FOR EUROPEAN HYBRID THREAT PREPAREDNESS 229
GÜVEN İÇÖZ* FAHRI ERENEL[2] BLUE CORRIDORS UNDER GREY-ZONE PRESSURE: OPERATIONAL LESSONS FOR MARITIME DEFENCE INNOVATION AND CRITICAL INFRASTRUCTURE RESILIENCE 230
RUTH KAILA* BUILDING MONETARY POWER THROUGH INFRASTRUCTURE: A NETWORK ANALYSIS OF CHINA'S DE-DOLLARISATION STRATEGY 231
SASU KATAJAMÄKI* CHINA'S RECENT DUAL-USE POLAR AND DEEP-SEA SCIENTIFIC ACTIVITIES IN THE ARCTIC: CAUSE FOR CONCERN FOR THE NORDICS? 232
DAVID MANNING* ROLAND HELLBERG[2] WARTIME SUPPLY CHAINS AND GEOPOLITICAL DISRUPTIONS: VULNERABILITIES, MACROECONOMIC TRANSMISSION, AND STRATEGIC RESILIENCE 233
JUHA MATTILA* RECOGNITION OF COMPETITIVE FORCES IN CONTEMPORARY EUROPEAN MILITARY STRATEGIES 234
MATTHEW MCGLYNN* THE FINANCIAL ARCHITECTURE BEHIND RUSSIAN SABOTAGE IN ESTONIA 235
LUKAS MILEVSKI* WOULD IT WORK ON US? THE GOLDEN QUESTION ABOUT EFFECT IN MILITARY THEORY 236
TIARNACH MOONEY* BEFORE THE WARNING: AMBIENT RESILIENCE BASELINE MONITORING AS A STRATEGIC INSTRUMENT AGAINST HYBRID THREAT EXPLOITATION 237
VLAD ONEȚIU* AI-AUGMENTED CIVILIAN COUNTER-INTELLIGENCE IN CYBER-ENABLED FINANCIAL WARFARE 238
ROLAND POPP* PREDICTING A 'PHONY WAR'?: HOW THE UNITED STATES-IRAN MILITARY CONFRONTATION EVOLVED INTO A PROTRACTED CONFLICT 239
STEPHEN SATKIEWICZ* THE GRAND DESIGN OF META-STRATEGY: THE NEXUS OF WAR, ORDER, AND IDEAS 240
DENNIS SULLIVAN* THE EGGSHELL MATRYOSHKA: NESTED COHERENCE DECAY, NUCLEAR SIGNALING AS LIMBIC HIJACK, AND THE LIMITS OF WESTPHALIAN DETERRENCE 241
NINA-MARI TAYLOR* THE IMPACT OF THE RUSSIA-UKRAINE CONFLICT ON FERTILISER DEPENDENCY AND FOOD SECURITY IN AFRICA 242
SANDRO TEIXEIRA MOITA* AGE OF FAILED CAMPAIGNS: IS IT STILL POSSIBLE TO RECONCILE OPERATIONS WITH STRATEGY? 243
ANZELA TITOVA* COGNITIVE WARFARE = NEUROLOGICAL MANIPULATION OF PERCEPTION IN THE DIGITAL AGE (CASE STUDY: RUSSIA'S STRATEGIC COMMUNICATION IN LATVIA DURING THE COVID-19 PANDEMIC) 244
GRACE TOVKACH* RETHINKING 'FROZEN' CONFLICT IN GEORGIA AND MOLDOVA: PROTRACTED EXHAUSTION STRATEGY AND IMPLICATIONS FOR WAR TERMINATION 245
MAKSIM VASSIN* RUSSIA: FRIEND OR FOE? CONSTRUCTION OF THREAT PERCEPTION AMONG ETHNIC RUSSIANS IN ESTONIA 246
ILZE VILKA* SOCIETAL RESILIENCE AS A WILL TO RESIST: A MULTI-LEVEL FRAMEWORK FOR SMALL FRONTLINE DEMOCRACIES 247

CHRISTINE WHITTAKER* SYSTEMIC INTERDICTION: OPERATION STARVATION AND THE ENDURING LOGIC OF STRATEGIC DENIAL 248
SHANG-SU WU* CAMBODIA AND THAILAND: COMPARISON OF MILITARY MODERNIZATION 249
SHANG-SU WU* LESSONS OF THE MIDDLE EAST WAR FOR TAIWAN 250
KONSTANTINOS XYPOLYTOS* FROM DECISIVE BATTLE TO ENDURING FORCE: UTILITY, ACCESSIBILITY, AND THE PROLIFERATION OF WAR 251

FOREWORD

Welcome to the ISMS Conference 2026, and welcome to Tartu.

This year's theme, *Military Sciences in Action: From Operational Insights to Defence Innovation*, describes a complex journey. Operations produce insights fast, and we are under constant pressure to turn them into new capabilities, doctrine and teaching. Academic rigour is slower, and it cannot be hurried without losing its value. Yet it is rigour that tells us whether an insight is a lesson or only an anecdote, and whether an innovation is an improvement or only a novelty. As professional military education institutions, we are asked to deliver speed and rigour at once. I do not think this tension can be fully resolved, but I do think we must keep trying to reconcile the two as best we can.

The interest this year has been remarkable. With more than 150 presentations and over 200 registered guests, the numbers show how much this work matters and how much our community wants a serious forum for it.

ISMS was founded by defence education institutions on the conviction that the military arts and sciences deserve academic attention in their own right. The society now spans everything from war studies and military history to technology, law and defence economics. That breadth is a strength. Today's problems rarely fit within a single discipline, and our work should not either.

Tartu is an unusual place, and a very fitting one for this conference. It is a university town in the classical sense, where scholarship has been pursued since 1632, and at the same time, a place where military education is part of daily life, home to both the Estonian Military Academy and the Baltic Defence College. The old academic tradition and the profession of arms share the same streets. That is rare, and it is the right setting for the questions we will discuss.

Leafing through this booklet, I am glad to see many names that return to ISMS year after year, and just as glad to see many that are new. Familiar voices give us continuity and depth, new voices bring fresh questions, and the meeting of different disciplines is where academic inquiry is at its best.

ISMS meets once a year, but the conversation does not stop in between. The presentations in this programme are only the visible part of a discussion that goes on all year, in classrooms, in research projects, in emails and in corridors, carried by people who keep at it without fanfare. Tartu gives us a few days to bring it into one shared space. Let us use them well.

This conference exists because of the institutional commitment of the ISMS member organisations, the persistence and good humour of our individual members, and the conference organising team at the Baltic Defence College. Thank you, all of you.

Welcome to ISMS 2026.

Tiia-Triin Truusa
President, International Society for Military Sciences
Dean, Baltic Defence College

WORKING GROUP 1:
WAR STUDIES

Chair

MARZENA ZAKOWSKA
National Defence University of Warsaw

Co-Chair

WILLIAM 'BILL' COMBES
Baltic Defence College

ISRAEL ALVES DE SOUZA JÚNIOR*

CHILD SOLDIERS: FROM PARAGUAY WAR TO CYBERSPACE

*Brazilian Army Command and General-Staff College (ECEME)

This is an investigation on child soldiers. The topic is delimited to the presence of child soldiers in the cyber domain. To carry out this research, the author posed the following question: As a result of the participation in the Paraguay War, how does the presence of children in cyberspace affect cyber warfare? This work was driven by the need to understand the effects of child-youth participation in actions in cyberspace, the diffusion of cyber power, and its consequences for society. Thus, the main objective is to understand cyberspace and the impact of the participation of child soldiers on this new domain.

Keywords: cyberspace, child soldiers, warfare, regulations, power

JAHANGIR ARASLI*

THE CASPIAN GATEWAYS: ASSESSING SECURITY THREATS, RISKS, AND CHALLENGES IN THE MARITIME DOMAIN

* Institute for Development & Diplomacy at the ADA University

One of the facets of the fraying world order is the advent of the strategic alignment between two revisionist anti-Western powers – Russia and Iran. Their territorial configuration virtually dissects the Eurasian landmass north to south, from the Arctic Ocean to the Persian Gulf. The only opening in this divide that provides a reliable East-West gateway is the Caspian Sea. Due to the post-2022 geopolitical shifts, it has emerged as a nexus of strategic energy, trade, and digital corridors that are of paramount significance for the littoral states and out-of-region stakeholders.

Against that backdrop, the Caspian Sea is becoming increasingly militarized. Russia and Iran exploit it as the only direct avenue of communication. Russia uses the waters and airspace to attack Ukraine with cruise missiles, while Ukraine gradually amplifies its long-range counterstrikes against Russian military facilities, warships, and offshore oil and gas infrastructure located in the Caspian Sea. During the recent Gulf War, Israel destroyed Iran's Caspian Sea naval base.

The Caspian Sea maritime domain has emerged as a vulnerable area. Both Russia and Iran have the capability sets, aptitude, and, potentially, political will to disrupt Western interests through the use of hybrid/asymmetric methods in a hypothetical conflict scenario. Iran has a proficiency in unconventional naval insurgency-type warfare, as demonstrated during the 2026 Gulf War. Russia, in turn, has a mastery of underwater (subsea) operations, which it now conducts in European waters. Given the Caspian Sea's compact geography and overcrowded critical infrastructure, this area offers a permissive environment for covert subversive activities and kinetic attacks (e.g., to disrupt Europe's energy supply chain).

Therefore, this presentation provides an analysis of the strategic environment in the region; a breakdown of the capabilities of the revisionist actors; an assessment of threats, risks, and challenges in the Caspian maritime domain; and brief recommendations.

Keywords: Caspian Sea, Russia, Iran, maritime domain, hybrid threats

PETTERI BLOMVALL*

POSTMODERN FIELD MANUAL - A TOOLBOX FOR FRAME-AWARENESS AND SITUATION-DEPENDENT TEMPO OF INNOVATION

*Finnish National Defence University

The fast pace of change on battlefields and in operations requires a fast pace of change among actors. This abstract argues that this requires adaptation as a minimum, but rather innovation and search for paradigmatic surprises. For this purpose, the abstract suggests a cognitive toolbox to facilitate sense-making and operational tempo.

Adaptation is seen as closing an experienced capability gap (Nisser 2026). This is seen as distinct from innovation, which builds something unprecedented and creates new gaps. At the end of this spectrum, there can be seen paradigm-shattering surprises (Liikola & Blomvall 2025). There is, of course, also risk included in unprecedented solutions. Innovation is seen as a high-reward marginal methodology compared to established best practices or adaptation when the situation demands.

The base of this toolbox is formed out of critical operational thinking, or the philosophy of operational arts, built on postmodernism. Critical postmodern philosophy is seen as a way to consciously bring up underlying assumptions, *epistēmēs,* and metanarratives to be challenged. This follows the reflective logics of the military design movement. A meta-toolbox of reflection can be seen emerging from several paradigms of operational arts: techno-rationalism, traditionalism, empiricism, systems thinking, and design thinking (Blomvall, forthcoming).

The concrete part of the toolbox builds on the Cynefin framework, which divides the encountered environments as systemically simple, complicated, complex, and chaotic (Snowden & Boone 2007). Distinct military organizational theories as well as military planning and design processes, are suggested for each quadrant. The toolbox suggests that one's own rate of change can be taken not just to the same systemic realm but to a higher one. Innovation and surprises are facilitated when one's own rate of change is pushed to the next quadrant compared to the enemy (Blomvall & Hirvi 2024; Blomvall 2024).

Keywords: operational art, innovation, adaptation, postmodernism

POPA BRINDUSA*

FROM HYBRID THREATS TO DEFENCE TRANSFORMATION: STRATEGIC COMMUNICATION AND SOCIETAL RESILIENCE IN CONTEMPORARY CONFLICT

*National Defence University 'Carol I', Regional Department of Defense Resources Management Studies (DRESMARA)

Contemporary conflicts increasingly demonstrate that the information domain has become a central arena of strategic competition, where state and non-state actors employ hybrid campaigns combining military pressure with disinformation, psychological operations, and influence activities. These campaigns increasingly target societal vulnerabilities, aiming to undermine public trust, weaken institutional legitimacy, and erode social cohesion. In this context, societal resilience has emerged not only as a societal objective but also as an essential defence capability requiring institutional adaptation.

This paper examines the role of strategic communication (STRATCOM) in strengthening societal resilience against hybrid campaigns and explores its implications for defence transformation. It argues that resilience within the information domain should be integrated into defence planning, capability development, and professional military education. Drawing on lessons from contemporary conflicts and recent security developments in the Euro-Atlantic environment, including experiences from Ukraine and the Baltic states, the study develops a conceptual framework linking hybrid campaigns, strategic communication mechanisms, and societal resilience.

The analysis suggests that coordinated communication strategies, institutional credibility, and public engagement can reduce the effectiveness of disinformation and strengthen societies' capacity to resist information manipulation. Furthermore, the paper highlights the need for defence institutions to adapt organizational structures, strengthen STRATCOM capabilities, and integrate information resilience into defence management and military education systems. By connecting lessons from contemporary conflicts with evolving defence practices, the study contributes to broader discussions on defence transformation in increasingly complex security environments.

Keywords: societal resilience, strategic communication, hybrid campaigns, defence transformation, information domain, hybrid threats

ANDRE CARVALHO*

OPERATIONAL ART IN THE AGE OF MACHINE REASONING

*Brazilian Army Command and General-Staff College (ECEME)

The increasing integration of AI-enabled systems and autonomous platforms into contemporary operations has renewed calls for a revolution in operational art, echoing earlier RMA thinking with its emphasis on speed, precision, and automated decision-making. This presentation critically engages with such claims, arguing that machine reasoning generates unprecedented risks to the very art that defines operational art. Drawing on a theoretical-conceptual framework, we examine how AI affects decision cycles, command relationships, and operational tempo. While automation may enhance efficiency in tactical sequencing, excessive 'platform-reliance' risks reducing warfare to targeting and attrition, stripping it of the judgment, creativity, and adaptability that operational art demands. No algorithmic system can substitute for the commander's capacity to understand ambiguous environments and exercise reasoned judgment.

Central to this argument is the practice of command itself. Operational art requires commanders and general staffs to advise and explain decisions under deep uncertainty. The art resides precisely in the capacity to act creatively and innovatively vis-à-vis ambiguity and imprecision. AI systems can calculate, but they cannot judge. Human-machine teaming and meaningful human control are therefore not exclusively dependent on humans being in/on the loop, but on commanders and staff officers thinking logically along intelligent systems. This study advances a conceptual framework for preserving operational art as a fundamentally human endeavour. Rather than prescribing a fixed model for AI integration, it identifies orienting parameters to harness AI as a force multiplier without surrendering the irreducible art of command. The implications are doctrinal as much as they are conceptual: as AI systems become further embedded in operations, the cultivation of human reasoning must remain the organising imperative of command education and staff development.

Keywords: operational art, artificial intelligence, command, operations

MIKE CRONIN*

IMAGINARIES OF THE RUSSO-UKRAINIAN WAR: FOLK THEORIES, CONSPIRACY NARRATIVES, AND RUSSIAN DISINFORMATION AMONG US CONSERVATIVES

*University of Tartu

When Trump and Vance attacked Zelensky in the Oval Office in 2025, many American conservatives applauded the action as the president standing up to an ungrateful ally. Meanwhile, the Trump administration continues to accommodate Putin, has refused to seek new US-funded military aid for Ukraine, has dismantled the US counter-disinformation infrastructure, and has ignored more than 18 incursions into NATO airspace by Russia since 2025.

This qualitative study asks: How do folk, disinformation, and conspiracy theories held by American conservatives shape their imaginaries about the Russo-Ukrainian War; what role does the received messaging from the Trump administration play in this? Semi-structured interviews with 32 self-identified political conservatives, conducted October 2024–December 2025, comprise the dataset. Those interviews revealed study participants' news sources, within an information environment dominated by conservative TV channels, podcasts, and algorithmic social media feeds where mainstream news organisations are widely distrusted.

Two audience-side mechanisms emerge from analysis through Simion's (2024) innovative redefinition and new taxonomy of disinformation, as well as Nguyen's (2018, 2022) description of epistemic bubble, echo chamber, and trust dynamics. *Concept hijacking* redefines "Russian disinformation" as a Democratic partisan weapon, with conservatives citing domestic political controversies such as the Steele dossier. *Ambient absorption without attribution* delivers Kremlin-origin messages and campaigns into participants' reasoning unsourced: NATO expansion provoked Russia's 2022 full-scale invasion; Ukraine is corrupt and a money-laundering dump; Zelensky panhandles for aid while dressed as a soldier and absconds with US funds; the war is a proxy fight enriching the US military-industrial complex; aid is a financial sinkhole. Many participants report hearing little from Russia while parroting Putin narratives as their own analysis. Recognition failure inside US conservative audiences is itself a national-security cost.

Keywords: Russian disinformation, folk theories, conspiracy theories, US conservatives, Ukraine

ŁUKASZ CUDNY*

IS THE KALININGRAD REGION RUSSIA'S STRATEGIC SECURITY HUB? TECHNOLOGICAL CAPABILITIES, A2/AD STRATEGY, AND THE TRANSFORMATION OF BALTIC SECURITY

*The International Association of Defence Products Manufacturers

The Kaliningrad region occupies a pivotal position in the Russian Federation's security and defence policy. Located between Poland and Lithuania, the exclave has evolved into one of Russia's most strategically significant military outposts, enabling the projection of military power across the Baltic Sea region. Since the annexation of Crimea in 2014 and, particularly, following Russia's full-scale invasion of Ukraine in 2022, Kaliningrad has become a cornerstone of Russia's regional deterrence posture and a key instrument for shaping security on NATO's north-eastern flank.

This paper examines the strategic role of the Kaliningrad region within contemporary Russian security and defence policy and analyses its implications for the evolving security architecture of the Baltic region. Drawing on Russian strategic documents, NATO policy papers, academic literature, and recent operational case studies, it investigates how military capabilities stationed in Kaliningrad – including the Baltic Fleet, integrated air and missile defence systems, long-range precision strike assets, and electronic warfare capabilities – support Russia's objectives of deterrence, power projection, and political coercion.

The paper argues that Kaliningrad should be understood not merely as an anti-access/area-denial (A2/AD) enclave but as a multidomain security hub integrating conventional military capabilities with hybrid instruments of influence. Recent incidents of GPS and GNSS interference affecting civilian aviation, maritime navigation, and NATO military operations demonstrate how electronic warfare complements conventional capabilities in shaping the regional security environment below the threshold of armed conflict.

The study concludes that Kaliningrad's growing strategic importance has accelerated changes in NATO's regional defence posture, strengthened security cooperation among the Baltic states, Poland, and the Nordic countries, and increased emphasis on resilience, multidomain operations, and critical infrastructure protection. By linking Russian security policy with operational developments in the Baltic theatre, the paper contributes to current debates on regional security, deterrence, and defence policy in Northern Europe.

Keywords: Kaliningrad, Baltic security, electronic warfare, military deterrence

FABRIZIO DE LONGIS*

THE NEW CYBER-AI COGNITIVE WARFARE

*Istituto Ricerche Studi Informazioni Difesa (ISTRID, Institute for Research, Studies, Information and Defence)

The growing integration of multi-agent artificial intelligence into information ecosystems is reshaping conflict across cognitive, informational, and security domains. This paper argues that fragmented authority, degraded trust, and automated decision-making in multi-agent systems create systemic vulnerabilities that undermine the cognitive resilience of societies and states, with implications for national security and defense. Large-scale generative multi-agent systems increasingly produce and amplify content. Synthetic media, including deepfakes, erode verification, accelerate disinformation, and weaken sense-making. Combined with Multi-Agent Decision (MAD) systems – distributed architectures based on interaction and delegation, yet limited in authority, trust calibration, and accountability – these dynamics generate unpredictable environments that challenge governance and control. From a defense perspective, this signals the emergence of cyber-cognitive warfare, where MAD systems act as autonomous instruments of influence. Perception management and informational dominance become operational effects, reflecting a hybrid militarization of AI across civilian and military domains. Their diffusion across civilian infrastructure creates persistent and scalable vectors for adversarial influence. Their recursive adaptability introduces risks of systemic drift, reducing human oversight and alignment with command intent, while reinforcing biased decision patterns. This challenges decision-making frameworks such as the OODA loop. At the societal level, sustained exposure to synthetic information environments may degrade attention, trust, and decision reliability, posing a growing national security threat. The paper concludes that these dynamics define a new class of systemic risk, requiring a reconceptualization of resilience that integrates cognitive security, cybersecurity, and AI governance within national defense. The emerging cyber-AI cognitive warfare.

Keywords: artificial intelligence, cognitive war, OODA, defense, national security

AHMED HASHIM*

THE STRENGTHS AND WEAKNESSES OF THE IRANIAN PILLARS OF DETERRENCE (BAZDARANDEGI) AND DEFENSE (DEFA)

*Australian War College and Deakin University

The IRI, cognizant of its material and technological inferiority vis-à-vis its primary threats, the United States and Israel, but devoted to its concepts of self-sufficiency and resistance, developed a series of pillars of deterrence and defense since the early 2000s after the US invasions and occupations of both Afghanistan and Iraq, when it became clear to them that Iran would likely be the next target. The Iranian leadership, aided by think-tanks, defense universities, and the senior military leadership, developed comprehensive foundational strategic concepts with key pillars. These strategic concepts were strategic depth – (*omq-e-rahbordi*) and forward defense (*defa pishjelou*). Strategic depth was to expand Iran's defensive depth as far away from its borders as possible. Forward defense – material and military aid to allies and proxies – was the material wherewithal to solidify strategic depth. The pillars are: 1) Mind Games: Passive Defense and Resilience; Bytes, and Atoms; 2) Defense Industrial Base: The Quest for Science and Technology; 3) Axis of Resistance: Forward Defense in practice in the Arab world; 4) Conventional Capabilities: Ballistic Missiles and UAVs.

Once we analyze these pillars, the discussion moves on to their performance in the wars of June 2025 and February to the present, with a focus on their strengths and weaknesses in these wars and what the future holds. IRI chose to horizontally escalate its war, much to the befuddlement and surprise of the United States; this is a major miscalculation and underestimation of IRI thinking. We conclude with a discussion of the strengths and weaknesses of what I refer to as conventional asymmetric warfare, with a nod to the case of Taiwan.

Keywords: IRI, deterrence, defense, ballistic missiles

MIINA KAARKOSKI*

CONCEPTUALIZING COGNITIVE WARFARE: MILITARY AND SOCIETAL IMPLICATIONS OF NATO'S APPROACH

*Finnish Defence Research Agency

Cognitive warfare describes the expansion of warfare into a phenomenon that is more difficult to define than conventional warfare, as cognitive attacks may also occur below the threshold of armed conflict. The concept emphasizes broader societal perspectives beyond the military while also constituting a distinct dimension of warfare. NATO's concept of cognitive warfare (2025) describes the dynamics and mechanisms of cognitive warfare and outlines requirements for improving cognitive resilience and capabilities. Using publicly available sources, this presentation employs conceptual research to examine the character of warfare that NATO's concept of cognitive warfare represents and to discuss the changes in thinking that the concept requires of both society and the military. According to the concept, both the military and society must reconsider and define the meanings of resilience, deterrence, and cognitive superiority.

NATO's concept of cognitive warfare is based on a character of warfare in which an adversary seeks to generate effects not only in the physical and virtual dimensions, but increasingly also in the cognitive dimension across the continuum of conflict. Technological developments have provided adversaries with new and more effective tools, which can be combined with scientific knowledge of how individuals, groups, and societies function, and how their behavior can be influenced or manipulated. After elaborating the conceptualization of cognitive warfare, this presentation addresses three requirements that arise from it. First, a whole-of-society perspective on warfare is needed in order to adapt to the conditions of cognitive warfare. Second, there is a requirement for deterrence against cognitive attacks. Third, there is a requirement for pursuing cognitive superiority in order to outmatch the adversary. These three requirements and their implications are examined especially from the perspective of the armed forces. The Finnish context, including the conscription system and the comprehensive security model, is used to concretize the meaning of the whole-of-society approach.

Keywords: cognitive warfare, NATO, resilience, deterrence, cognitive superiority

PETER MEEDOM*

THE UKRAINE WAR AND THE CRISIS OF RUSSIAN MILITARY THOUGHT

*Royal Danish Defence College

The war in Ukraine has produced a crisis in Russian military thought. The initial campaign in February 2022 was premised on manoeuvre warfare by light, mobile forces, the primacy of noncontact and non-military instruments, and the concept of 'active defence' that had taken shape across the post-Serdyukov decade. Within weeks, it had collapsed into positional and attritional war, exposing both the misjudgement of Ukraine and the limits of the operational concepts that had guided Russian force development.

This paper examines how the war is reshaping Russian military thought at the interface between operational practice and strategic conception. Drawing on Russian-language primary sources, including doctrinal exchanges in *Voyennaya Mysl* and *Armeysky Standart*, strategic-level commentary by figures such as Trenin and Baluyevsky, and on recent scholarship (Jójárt 2024; Engqvist et al. 2025; Jonsson 2026; Watling 2026), it traces the reactivated debates: offence and defence, manoeuvre and position, and destruction and attrition. The connecting problem is the transparent battlefield, where saturation by drones and reconnaissance-strike complexes has eliminated the fog of war and made the concentration of forces near-impossible.

The paper argues that this operational transformation is reshaping the character of war. As the theatre becomes boundless, attrition is recast as a test of the resilience of entire political-economic systems, prosecuted through the integration of conventional fires, long-range strike, and the targeting of dual-use infrastructure. War and peace are increasingly held to coexist, with the conflict with the West understood as the strategic horizon. The implications extend beyond Ukraine: the Russian military emerging from this debate is one calibrated for protracted, multidimensional confrontation with NATO, while seeking the means by which manoeuvre, surprise, and decisive effect can again be made possible.

Keywords: Russia, Ukraine, military thought, transformation of warfare

EDUARDO XAVIER FERREIRA GLASER MIGON*
JARBAS ALFEU DE PAULA JUNIOR[2]

QUANTUM TECHNOLOGIES AND THE TRANSFORMATION OF WARFARE: INFORMATION SUPERIORITY, STRATEGIC COMPETITION, AND THE FUTURE OF MILITARY POWER

*Military Engineering Institute and Brazilian Army Command and General Staff College (ECEME), [2]Brazilian Army Command and General-Staff College (ECEME)

Quantum technologies are increasingly recognised as a disruptive frontier in strategic competition, yet their implications for warfare extend beyond discrete technological applications. This paper examines how quantum sensing, communications, and computing may collectively transform the informational foundations of military power and reshape the character of warfare in the coming decades. The central argument is that future warfare will be defined not only by the ability to generate force but also by the capacity to secure, interpret, and exploit information within a multidomain, contested information environment. In this context, quantum technologies introduce a structural shift in the basis of information security, moving from architectures grounded in computational hardness to approaches increasingly informed by physical principles. This transition does not imply immediate replacement of existing systems, but rather a growing tension between legacy infrastructures and emerging security paradigms. The analysis develops this argument through three interrelated pathways. First, quantum sensing enhances the fidelity and resilience of perception, enabling more robust positioning, navigation, timing, and detection in contested operational environments. Second, quantum-enabled communications introduce alternative models of securing information flows, while simultaneously exposing the long-term fragility of classical cryptographic systems and raising concerns regarding deferred exploitation of encrypted data. Third, quantum computing holds the potential to disrupt existing information-security architectures and expand capabilities in optimisation, simulation, and complex decision support. Rather than treating these developments as independent technological advances, the paper conceptualises them as elements of an ongoing transformation in the relationship between information, decision, and power in warfare. It introduces the notion of an informational asymmetry transition, in which states diverge in their ability to protect and exploit strategic data under conditions of technological change. The paper concludes that the most consequential impact of quantum technologies will not be immediate battlefield disruption, but the gradual reconfiguration of decision advantage, command resilience, and strategic autonomy.

Keywords: quantum technologies, information security, decision advantage, strategic autonomy, future warfare

OLENA PROKOPYSHYNA*

HOW THE OFFENSIVE RUSSIAN MILITARY OPERATION AGAINST UKRAINE HAS CHANGED OSINT

*University of Leicester

Open-source intelligence is considered one of the most accessible tools to track dynamics in war zones. During the armed conflict in Syria, OSINT was widely used to identify military units and their alleged commanders. Nevertheless, this type of conflict involved State actors, yet it is classified as a non-international armed conflict. It contributed to the OSINT tradecraft for civil actors but has limited influence on the military doctrine, per se.

In 2022, the full-scale invasion of the Russian Federation in Ukraine, considered as one of the biggest armed conflicts in Europe since the Second World War, has changed most of the military domains. In this paper, we briefly examine the development of OSINT as a tradecraft during the period of the beginning of the Russian aggression against Ukraine from 2014 to 2022. Then we focus on the specific patterns which emerged as tools during the ongoing Russian full-scale invasion. As a primary example, we discuss the tactics of the Russian Armed Forces, which challenges the OSINT tradecraft.

For years, measuring effective control, occupation, and liberation of contested territories in war zones has been done by analysing open-source materials from both sides of the armed conflict. However, the Russian Armed Forces sent a number of servicemen to film footage to circulate on social media, creating the impression that Russia was gaining territory; however, these territories were in the vicinity of armed conflict or were in the grey zone. Why was this challenging for OSINT practitioners? Because for basic verification, we have real clues, but the assessment of frontline dynamics by OSINT is contested.

Keywords: OSINT, warzone, Russian full-scale invasion

RIKKE MICHELLE RIETVELD*

BATTLEFIELD FORENSICS IN ACTION: FROM OPERATIONAL LESSONS TO AN INTEROPERABLE NATO CAPABILITY

*NATO and Cranfield University at Shrivenham Defence Academy

Modern conflict has shown that the scientific exploitation of battlefield-recovered material is no longer a niche technical activity. It can support intelligence, force protection, attribution, legal accountability, host-nation support, and the identification of the fallen. However, within NATO and many national structures, these activities are still often fragmented across technical exploitation, biometrics, battlefield evidence, intelligence, policing, legal, medical, and civilian forensic communities.

This presentation will introduce findings from my ongoing PhD study: The Past, Present, and Future of Battlefield Forensics. The study uses Action Research, supported by Grounded Theory, to examine how Battlefield Forensics can be better understood, coordinated, and implemented as a practical framework for NATO and partner nations. Drawing on operational experience, field observations, specialist interviews, NATO working groups, doctrine review, and workshop-based research, the presentation will show how the research has moved beyond theory and into practical implementation.

The presentation will discuss concrete outcomes already developed or initiated, including awareness training, specialist staff functions, standardised reporting, concept development, coordination mechanisms, and the testing of Technical Exploitation coordination during exercises. It will also address the remaining challenges: unclear terminology, fragmented responsibilities, legal uncertainty, limited national capacity, and the need to connect military, governmental, civilian, academic, and industry expertise more effectively.

Particular attention will be given to the relevance of Battlefield Forensics for small and medium-sized NATO nations, including the Baltic States. In a regional context shaped by hybrid threats, host-nation responsibilities, Article V planning, and proximity to ongoing conflict, Battlefield Forensics offers a practical way to strengthen resilience, interoperability, and decision-making.

The presentation will conclude with a proposed way ahead: common terminology, scalable coordination structures, training pathways, legal guidance, and a stronger Battlefield Forensics community of practice capable of supporting operations from grey-zone incidents to high-intensity conflict and post-conflict accountability.

Keywords: battlefield forensics, technical exploitation, battlefield evidence, NATO interoperability, civil-military cooperation

ANDRE SIMONYI*
YURIY NAPLYOKOV[2]

STRATEGIC TURBULENCE AND THE FUTURE OF OPERATIONAL PLANNING IN CONTEMPORARY CONDITIONS

*Royal Military College Canda-Saint-Jean, [2]Taras Shevchenko National University of Kyiv

The war in Ukraine has demonstrated that strategic turbulence and operational complexity are signs of a revolution in military affairs, a change in operational reality that forces the re-examination of current strategic and operational planning processes. New technologies and geopolitical realities accelerate the operational tempo, requiring a quicker and more agile planning process to achieve dominance at all levels. This emerging operational reality highlights a paradox: current planning processes based on NATO's OPP (Operational Planning Process) encounter wicked problems of a seemingly illogical nature, disrupting the forecasted flow of events. The classical paradigm of deductive, linear logic proves inadequate. The conduct of warfare in Ukraine is characterized by obsolete regulative rules and the absence of new ones. Planners at all levels need new planning tools.

Adapting to this new approach to thinking, planning, and organizing is potentially the main challenge facing our capacity to change. It requires a complex process encompassing a fundamental review of our decision-making and planning approaches that involves strong leadership to instil the required change. Such fundamental change requiring a review and deep adaptation of NATO's OPP towards a more adaptive and fluid process is met with institutional inertia resisting our current mental models that unconsciously regulate thinking in decision-making and behavior. However, failure to adopt a renewed vision, approach, and method for planning will limit the effectiveness of our strategic and operational capabilities in creating a competitive advantage in this new, complex environment.

In this paper, the authors expose the emerging, complex, and turbulent environment in which warfare is conducted. Without completely evacuating the NATO OPP, the authors discuss a renewed approach to the planning process required to respond to the fast-paced operational environment. They argue that to implement a new way of planning, mindset, freedom of thoughts, creativity, inter-level interaction, increased communication, managerial courage, and a proper organizational culture are indeed essential for its success.

Keywords: strategic turbulence, operational planning, operational complexity, military adaptation, Ukraine

THOMAS SLENSVIK*
ANDERS MCD SOOKERMANY[2]

WHAT HAPPENS WHEN SYSTEMS ORIENTED DESIGN MEETS MILITARY PLANNING? METHODOLOGICAL OBSERVATIONS FROM FOUR PLANNING WORKSHOPS

*Norwegian Defence University College, [2]Norwegian Defence University College, Command and Staff College

Contemporary military planning depends on doctrinal processes that provide coordination, interoperability, and momentum. Yet such processes can become difficult to adapt when planners face complex situations in which relationships, problem framings, and possible futures remain uncertain. This paper examines how military planning practice changes when officers engage in Systems Oriented Design (SOD) alongside established NATO-oriented planning conventions. The paper draws on four planning workshops conducted between 2023 and 2025 within joint operational planning contexts at the Norwegian Defence University College. The workshops involved groups of military officers working through an operational scenario using SOD-informed approaches, including giga-mapping, iterative visual exploration, scenario development, and adapted design tools. Empirical material includes workshop observations, facilitator fieldnotes, audio reflections, semi-structured interviews, and planning artefacts.

Rather than assessing SOD as a discrete method or measuring the quality of planning outputs, the paper investigates transformations in how planning work is organised and how understanding develops collectively. It asks: *What changes in planning practice when military officers use Systems Oriented Design?* Three dimensions are examined: the temporal structure of collaboration, the role of iteration in knowledge development, and the capacity to sustain divergence before converging on courses of action. Preliminary observations indicate that SOD can shift collaboration from episodic handovers between specialist contributions toward more continuous collective sense-making around shared visual artefacts. Iteration becomes less a correction of earlier work and more a means of discovering new aspects of the problem space. Sustained divergence, however, also produces moments of uncertainty in which participants may experience a loss of direction and seek to return to familiar procedural structures.

The paper argues that these developments should be understood as transformations of planning practice rather than as tool adoption. SOD is approached not primarily as a method, but as a systemic orientation toward complexity enacted through situated planning practices. The study contributes empirical insight into how complexity-oriented design approaches may alter collaboration, inquiry, and problem framing within military operational planning.

Keywords: military operational planning, Systems Oriented Design, joint operations, complexity, planning practice

MART SOONIK*
MAI BEILMANN[2]

THE DOMESTICATED FRONT LINE. CHILDREN'S WAR MEANING-MAKING AND COGNITIVE SECURITY IN A BORDERLAND STATE

*[-2] University of Tartu

Context: Societal resilience against hybrid threats and grey-zone activity depends not only on institutions, critical infrastructure, and adult populations, but also on the cognitive and affective dispositions formed before adulthood, through which children and adolescents learn to interpret threat, belonging, and safety. In Estonia, a NATO borderland state neighbouring Russia and marked by Estonian-, Russian-speaking, and Ukrainian community contexts, the war in Ukraine is near and socially present. Children encounter it through screens, classrooms, and family talk, yet defence research has rarely treated their meaning-making as part of cognitive security.

Purpose. The presentation introduces the domesticated front line, the process by which a proximate but non-arrived war is rescaled into children's everyday spaces and asks what the evidence base can and cannot tell us about the borderland child as a situated security subject.

Method. It draws on a critical interpretive synthesis of 27 empirical studies (1975–2025), screened across children's geographies, political socialisation, media studies, and developmental psychology, and read through four lenses: mediation, affective geographies, geopolitical imagination, and agency.

Findings. Home, school, and screens function as geopolitical sites rather than neutral channels. Children's fear, solidarity, and uncertainty are socially produced and may accumulate over time rather than peaking around discrete crises. The synthesis suggests that children in different ethnolinguistic communities may draw on different interpretive repertoires when making sense of war, belonging and safety. Yet the borderland child, where war is proximate, unresolved and ethnolinguistically divisive, remains largely absent from the empirical record.

Implications. The paper argues that children's war meaning making should be treated as an empirically traceable dimension of cognitive security and societal resilience, through which cognitive vulnerabilities take shape before adulthood. It specifies a research agenda for production-based, multilingual, cross-community studies with 11–14-year-olds that would connect critical geopolitics and childhood studies to defence debates on resilience and hybrid threats.

Keywords: cognitive security, societal resilience, hybrid threats, children of borderland, war meaning making

FRISO STEVENS*

ROOM FOR MANEUVER AFTER UKRAINE? TOWARD A TACTICAL DEFENSEORIENTED DOCTRINE FOR EUROPEAN NATO RESTORING SOME MOBILITY

*University of Oxford

This article argues that European land warfare doctrine should be amended through defense-oriented adaptations to be able to stop a Russian assault without the US, especially its C4ISR enablers that now form the backbone of NATO's information infrastructure. European defense establishments have long embraced the American offense-minded maneuvre doctrine that is premised on guaranteed air superiority, mobile mechanized firepower, and multi-domain operations that are guided by network-centric warfare capabilities. With the US security guarantee now uncertain, the article re-examines long-held assumptions in land warfare in light of rapid military-technological innovations in radar and drones on display in Ukraine today. Subsequently, the article spells out what a prudent military transformation of Europe's force structure could look like by drawing on Biddle's modern system of force employment. Specifically, the article works out viable defensive tactics (cover, concealment, dispersion, suppression, combined arms, and independent small unit maneuver) and operations (centered on depth, reserves, and counterattack).

Keywords: maneuver warfare, transparent battlefield, unmanned aerial vehicles, military transformation, Biddle's modern system

ADAM SVENDSEN*

THE VIRTUES OF INTELLIGENCE ENGINEERING (IE): HELPFUL AS A START FOR NAVIGATING UNCERTAINTY…

*Norwegian Defence University College (NDUC/FHS)

When generally navigating much uncertainty confronted by many different stakeholders, for instance, in the North Atlantic Treaty Organisation (NATO) and when confronting several emerging disruptive tech (EDT) environments across the conduct of many multi-domain operations (MDOs), this paper further advances the 'Intelligence Engineering' (IE) case.

Extending beyond merely its roots in the general disciplines of the 'arts' and the 'sciences', this paper contends that intelligence today is more about 'engineering'. That last 'engineering' work undertaken in the intelligence context also includes 'Federation-/System-of-Systems' and 'Team-of-Teams'-based 'architectural design processes', that are harnessed to even more innovative extents.

During its course and highlighting the example of contemporary Intelligence, Surveillance and Reconnaissance (ISR) work, in its conclusions, this paper argues that uncertainty is able to be navigated in a much more improved manner if the process of 'Intelligence Engineering' (IE) is better seized, featuring at least as a viable starting place for those efforts.

IE can then be combined or jointly deployed with a multitude of other approaches and methodologies, the most obvious being Structured Analytic Techniques (SATs), ranging to morphologically-informed Strategic Options Analysis (SOA) work, to better realise next steps and future course(s) of action going forward into a multitude of futures ahead.

Improved foresight is developed, providing better insight into uncertainty through further explicitly developing Foresight Intelligence ('FORINT'), as well as offering more 'information-' to 'decision-advantage' via the greater effective meeting of classic end-user STARC criteria, relating to: Specificity, Timeliness, Accuracy, Relevance and Clarity, in whatever is delivered to stakeholders.

Keywords: intelligence, intelligence engineering, foresight, uncertainty navigation

GONZALO VÁZQUEZ*

THE GRAY ZONE OF SEA POWER IN THE 21ST CENTURY: IMPLICATIONS FOR NATO

*Spanish Naval War College

The return of great power competition and its strategic effects at sea have materialized in the proliferation of hybrid tactics and operations in the gray zone. Such tactics, which seek to heighten uncertainty in the maritime environment and complicate both attribution and effective response, are gradually increasing the costs of the naval presence required to protect vital SLOCs and critical undersea infrastructure.

This paper explores the gray zone dimension of sea power in the 21st century and its growing strategic relevance to NATO allies. In so doing, it first provides a theoretical framework for gray zone operations and hybrid strategies to contextualize recent events, framing the gray zone as an escalation regime rather than a mere catalogue of hybrid instruments. It follows with an analysis of the most significant events that have taken place over the last decade, linking them to the previously described logic. It then delves into the most significant implications for allied nations and the way in which this new reality is affecting – and will continue to affect – NATO's posture at sea.

The central contention is that the hybrid dimension of sea power and maritime operations in the gray zone will continue to gain prominence in the coming years, imposing additional demands and a need for further adaptation for the Alliance's maritime posture. The Baltic, North Atlantic, and Mediterranean will become central arenas of this asymmetric competition between NATO and Russia, while China will continue to pose a more overt risk both in the waters of East Asia and with the development of its dual-use infrastructure.

Keywords: sea power, maritime strategy, gray zone, hybrid threats

STEPAN YAKYMIAK*

ROBOTIZATION OF WAR: IRREVERSIBLE SHIFTS IN THE DEFENSE ECOSYSTEMS, MILITARY SCIENCE, AND EDUCATION

*Centre for Defence Strategies

The speech, based on an analysis of the Ukrainian experience of robotization of military operations and global trends, will consider changes in the requirements for defense ecosystems, military science, and education on the following issues: Robotization of war: Ukrainian experience, global trends, future concepts, and defense ecosystems; challenges of robotization and military science: updating known and forming new knowledge; and the impact of robotic warfare on the requirements for military education.

Keywords: robotization of war, robotic systems, defense ecosystem, military science, military education

MARZENA ZAKOWSKA*

BELOW THE THRESHOLD OF WAR: HYBRID PRESSURE AND CONTROLLED ESCALATION IN KOSOVO (2016–2026)

*War Studies University

This article analyses the most recent phase of the Kosovo conflict (2016–2026) as a hybrid conflict, in which the unresolved dispute over Kosovo's status becomes a deliberately exploited instrument of strategic influence operating below the threshold of open war. Its central argument is that, once the international stabilisation system built after 1999 entrenched the non-resolution of Kosovo's status, the unresolved conflict itself became a useful strategic resource. The article, therefore, asks: how is the non-resolution of Kosovo's status turned into an instrument of hybrid pressure that stays below the threshold of open war?

The study shows how political, diplomatic, informational, paramilitary, and institutional means are combined into a single mechanism of pressure. Hybridisation is therefore neither sudden nor autonomous, but rather a structural consequence of the unresolved status and a continuation of earlier rivalry, in which the Serb community of northern Kosovo becomes an instrument of strategic influence.

Theoretically, the study draws on the concepts of hybrid warfare and the grey zone.

Methodologically, it is a qualitative single-case study embedded in a realist framework. Empirically, it reconstructs a coherent sequence of events: 2016–2017 mark the shift from managing the conflict to exploiting it; 2018–2021 see a diplomatic offensive and a 'narrative war', including the 2018 transformation of the Kosovo Security Force into a regular army; 2022–2023 bring the licence-plate crisis and the withdrawal of northern Serbs from Kosovo's police, judiciary and administration, demonstrating the capacity to paralyse the state without open war; 2023 brings proxy violence, culminating in the Banjska attack; and 2024–2026 form a phase of chronic conflict and apparent stabilisation, in which tension becomes a new 'normal'.

The study concludes that Kosovo functions as a durable hybrid system operating under formal peace and introduces a new category – 'managed hybrid conflict'.

Keywords: Kosovo, Serbia, hybrid conflict/warfare, grey zone, managed conflict, North Kosovo, below the threshold of war

AGNIETE ZOTKEVICIUTE BANEVICIENE*

TURNING WEAKNESS INTO DETERRENCE: THE LOGIC OF STRATEGIC EXPOSURE (PART I)

*General Jonas Žemaitis Military Academy of Lithuania

Classical deterrence emphasises denial and punishment – strategies that small states cannot autonomously deliver. This presentation introduces *strategic exposure* as a conceptual innovation within extended deterrence: the deliberate publicisation of vulnerabilities and dependencies to shape adversarial expectations indirectly through alliance dynamics. It develops a theoretical framework specifying three core mechanisms – performed vulnerability, reputational binding, and normative framing – through which exposure transforms perceived weakness into a strategic asset. The presentation also identifies key scope conditions for effectiveness, including alliance cohesion, credible normative alignment, and disciplined messaging. By reconceptualising vulnerability as a tool rather than a liability, the argument advances a relational understanding of deterrence in asymmetric security environments.

Keywords: strategic exposure, deterrence theory, small states deterrence, alliance politics, reputational binding, normative framing, performed vulnerability

AGNIETE ZOTKEVICIUTE BANEVICIENE*

STRATEGIC EXPOSURE AS A DETERRENCE-AMPLIFYING MECHANISM IN LITHUANIA'S NATO POSTURE (PART II)

*General Jonas Žemaitis Military Academy of Lithuania

Building on the concept of strategic exposure, this presentation examines its empirical application in Lithuania's NATO posture between 2022 and 2025. Using directed qualitative content analysis and process tracing of doctrinal texts and elite statements, it demonstrates how Lithuania publicly articulates vulnerability to mobilise alliance interdependence and frame defence as a shared responsibility. The analysis shows how strategic exposure contributes to shaping expectations about the speed, credibility, and political resolve of NATO reinforcement. The findings suggest that this mechanism can accelerate the effects of denial and punishment when commitments are institutionally anchored, but may also generate risks of backfiring when alliance cohesion is contested. The study clarifies how managed visibility operates in practice as a deterrence-amplifying strategy in asymmetric contexts.

Keywords: strategic exposure, deterrence theory, small states deterrence, alliance politics, reputational binding, normative framing, performed vulnerability

WORKING GROUP 2:
MILITARY HISTORY

Chair

ART JOHANSON
Baltic Defence College

Co-Chair

RANNO SÕNUM
Estonian War Museum

GREGOR DE ROOY*
HÉLIO FARIAS[2]

FROM THE FIELD TO THE CURRICULA, A STUDY OF PERCEIVED THREAT AND INTELLECTUAL RESPONSES FROM BRAZILIAN GENERALS

*-[2]Brazilian Army Command and General-Staff College (ECEME)

This research sheds light on how civil and international conflicts, such as those from the late 19th and early 20th centuries, as well as the First and Second World Wars, impacted the curricula of the Brazilian Superior School of War, founded in 1949. Based on the hypothesis that field experience influenced the thinking of key officials, who later had the means to shape the curricula of the Superior School of War, this study adopts a qualitative approach. It analyzes the bibliographies and biographies of authors from two significant intellectual streams within the Brazilian Army: the National Security authors and the Geopolitics authors. Namely marshals Goes Monteiro and Mario Travassos as well as generals Lyra Tavares, Juarez Távora, Francisco de Paula Cidade, Golbery do Couto e Silva, and Meira Mattos. Subsequently, the research examines the curricula of the Brazilian Superior School of War, through on-site archival research, to assess whether their ideas, drawn from their writings and military experiences, are reflected in the School's curricula. This research utilizes the theoretical framework of constructivism, which posits that ideas are central to institutions and are mutually constructed among actors and institutions.

Keywords: geopolitics, Brazil, national security, curricula

JOSEPHINE DURANT*

PASSING FOR LOCAL IN WWII OCCUPIED FRANCE: THE STRATEGIES OF F SECTION FEMALE SPIES

*Oxford University

This presentation examines the strategic use of gender as an instrument of irregular warfare through the example of women spies from the Special Operations Executive (SOE). This WWII British secret service hired women as field agents in an unprecedented transgression of mid-20th century gender norms. Most SOE women worked for F Section, which sent French-speaking but non-French agents to Nazi Occupied France. There, spies took part in intelligence gathering, sabotage, and counter-propaganda missions while passing for local civilians. Despite their lack of previous espionage experience, archival sources suggest that most of F Section's 39 women escaped enemy detection.

Using historical and sociological data, this project argues that SOE women weaponised their gender to mimic French civilians. They strategically exploited the misogynistic assumptions of German Occupiers, who underestimated women, and combined three types of signalling to pass for compliant locals. Institutional signalling involved SOE drawing upon stereotypes of feminine harmlessness to create credible cover stories. Improvised signalling occurred when women put on impromptu performances to signal chosen qualities, including flirtatiousness and weakness, to enemy Germans. Finally, socially learnt signalling featured agents correcting each other's spoken French, as well as the monitoring of superficial signals (such as identity papers, mannerisms, and physical appearance) by local resisters.

By framing gender as a crucial part of women spies' signalling, this historical case study generates broader insights about the future of warfare and its gendered dynamics. Indeed, modern intelligence operations, such as the ongoing Russian "Illegals" programme in the US, still rely on deep-cover operatives. However, the use of gender-based strategies by spies and their wider place in contemporary conflicts remain overlooked, making the case of SOE women worth revisiting today.

Keywords: espionage, gender, identity

LENE EKHAUGEN*

NORWEGIAN UN PEACEKEEPERS AND LEISURE IN GAZA: 'FOR BENEFIT AND ENJOYMENT'

*Norwegian Defence University College

Approximately 11,000 Norwegians served in the United Nations Emergency Force (UNEF) between 1956 and 1967. As part of a broader study of Norway's participation in the operation, this paper explores the soldiers' "leisure time". The management of the soldiers' leisure time illustrates which priorities were considered important alongside their service as peacekeepers. "Free time" was not truly "free", but rather a void that was to be filled with useful activities. According to a contingent commander, emphasis had been placed on giving personnel 'the opportunity to make use of their leisure time in ways that would be to their benefit and enjoyment', (DANOR VII, author's translation). Drawing on end-of-tour reports, records, interviews with veterans conducted in 2025/2026, and existing literature, this paper explores evolving leisure time activities during the 11-year period and tentatively argues that efforts were made to keep the soldiers occupied for three main reasons. First, during the first five contingents, most personnel were conscripts. They were therefore to be engaged in sports and training, so that, upon returning to Norway, they could function within the Norwegian invasion defence structure. Second, leisure time was seen as a potential source of unrest, making it important to keep personnel occupied. Third, filling soldiers' free time with structured activities aligned with broader norms in the Norwegian society at the time.

Keywords: UNEF, DANOR, leisure time

MILENA ALICIA JAKSIC*

FROM OPERATIONAL INTEGRATION TO MULTI-DOMAIN OPERATIONS: HISTORICAL LESSONS FROM LUFTWAFFE OPERATIONAL ART

*University of Potsdam and School of Advanced Air and Space Studies

Contemporary discussions on MDO frequently emphasize technological enablers such as AI, autonomous systems, and advanced networking architectures. This paper argues that MDO's central challenge is fundamentally operational rather than technological and should be understood as the latest manifestation of a longstanding military problem: the integration of military effects under conditions of uncertainty, friction, and organizational constraint.

Rather than representing a revolutionary break with previous military thought, MDO is examined as part of an evolutionary continuum extending from Air-Land Battle through Joint Operations, Effects-Based Operations, and Full Spectrum Operations. From this perspective, contemporary force design challenges are less concerned with inventing entirely new methods of warfare than with adapting enduring operational principles to emerging technological environments.

Drawing upon the Luftwaffe's operational art during World War II, the paper examines one of the earliest attempts to synchronize effects across multiple dimensions within a unified operational framework. While Germany ultimately failed to translate operational success into strategic victory, the Luftwaffe's experience offers valuable insights into the enduring requirements and limitations of multi-domain warfare. The paper treats operational airpower not as a doctrinal precursor to MDO, but as an early case study in the integration of military effects across three dimensions and all levels of war.

The study identifies six recurring operational mechanisms: (1) integration of effects across domains, (2) acceleration of operational tempo, (3) deep interdiction and systems disruption, (4) decentralized execution through mission command, (5) simultaneous employment of airpower capabilities across multiple levels of war, and (6) structural depth and sustainability.

These mechanisms are assessed against contemporary MDO and JADC2 concepts to evaluate which historical principles remain relevant to contemporary warfare and force design. The paper concludes that enduring principles of operational integration continue to shape military effectiveness and must be translated into contemporary organizational and doctrinal frameworks if MDO is to fulfil its promise as a warfighting concept.

Keywords: multi-domain operations, operational art, airpower, operational integration, force design

THOMAS M. JAMISON*

WAR STORIES: MILITARY FICTION AND PREPARATION FOR FUTURE WARS AS HISTORICAL CASES

*Naval Postgraduate School

People spend a great deal of energy forecasting the future of war. Alongside war games and modelling, a popular tool for this task is the "future war story": imagined conflicts informed by detailed assessments of current and/or future military capabilities. The genre tends to flourish under conditions of radical technological change and "Great Power" peace punctuated by regional or civil wars that demonstrate the potential of new weapons. There have been three "golden ages" of "future war stories" motivated by these technical and political circumstances: the Victorian "Long Peace" in the late-nineteenth century, the Cold War during the 1970s and 80s, and, beginning in the 2010s, "Great Power Competition" with the People's Republic of China (PRC).

This essay compares future war stories in the Anglo-American experience from the Victorian period, the late-Cold War, and the present. Appreciating the durability of the format will sensitize consumers against the dangers and opportunities of fiction, and by extension war forecasts more generally. War fiction is useful as a tool for conceptual development, ideological struggles within services, and the generation of war game scenarios. Nonetheless, as this paper argues, the genre tends to recreate three fallacies across eras and technological ruptures: that future wars will be decisively decided in a comparatively short timespan; that novel technologies will achieve said decision; and that third-party states (even when they constitute the battlefield itself) have only limited agency.

Keywords: fiction, military history, predictions

PERIHAN KARADEMIR*

OPERATIONAL ADAPTATION IN STEPPE WARFARE: FOUNDATIONS OF MONGOL MILITARY SUCCESS

*National Defence University (Türkiye)

The successes of the Mongol military system are attributed to factors such as high mobility, advanced archery skills, leadership, and discipline. However, these factors alone are insufficient to explain how a steppe-based military system could sustain its military effectiveness across diverse geographical conditions and battlefields stretching from China to Central Europe. In response, this study does not aim to revisit the military campaigns organized by the Mongols, but rather to examine the fundamental components of military effectiveness by taking the Mongol military system as a case study. The central question of the study is how the Mongol military system sustained its effectiveness across diverse operational environments, particularly relative to other contemporary military systems, and what these reveal about operational adaptation.

The study focuses on five key factors that shaped Mongol military success: operational mobility, intelligence and reconnaissance, the chain of command, psychological warfare tactics, and the ability to adapt to diverse operational environments. The study aims to analyze how these elements interact and integrate within a system that generates military effectiveness by evaluating Mongol campaigns conducted under varying climatic, environmental, geographical, and political conditions. In particular, the study examines the information-gathering and assessment processes of the steppe military system, its flexible command structures, high level of maneuverability and mobility, communication networks, and the coordinated use of different military elements towards a common operational objective.

Furthermore, the study argues that Mongol military success was not based on a specific weapon system, tactic, or technological superiority; rather, it was the result of a military structure capable of adapting to different geographies and operational conditions. In this context, the Mongol example demonstrates that military effectiveness arises not from a single superior element but from the combination of mobility, information superiority, command flexibility, psychological impact, and operational adaptability.

In conclusion, this study aims to explain how military organizations maintain their effectiveness amid changing operational conditions through a historical case study and to contribute to the broader discussion about the fundamental components of military effectiveness.

Keywords: steppe warfare, operational adaptation, intelligence, Mongol warfare, military effectiveness

JAKUB MAŁOLEPSZY*

INTERWAR POLISH COUNTER-SABOTAGE EFFORTS AGAINST THE SOVIET UNION AS LESSONS FOR MODERN HYBRID THREATS ON NATO'S EASTERN FLANK

*Jan Dlugosz University in Czestochowa

One of the greatest threats to security in Europe today is the Russian Federation's aggressive policy. At present, the most serious danger to European security comes from various forms of hybrid warfare conducted by Russia. These activities include sabotage attacks on critical infrastructure, cyberattacks, and disinformation campaigns aimed at destabilizing European societies and institutions. The countries that are most exposed to Russian hybrid activities are undoubtedly Poland and the Baltic States. All four states place enormous importance on strengthening their national security and resilience against potential threats. In recent years, they have undertaken significant efforts to create systems and defensive measures intended to limit the effectiveness of hybrid operations on their territories. To prepare effectively to respond to Russian hybrid attacks, it is important to look to history and draw lessons from similar situations. One of the best historical examples can be found in the actions of Polish security services, especially the Border Protection Corps (*Korpus Ochrony Pogranicza*), against Soviet diversionary and sabotage operations on the eastern borders of Poland during the interwar period. This example is significant for several reasons. First of all, it serves as an excellent case study showing how Russian and Soviet concepts of diversionary warfare developed over time. It also demonstrates how the Polish state reacted to threats coming from the Soviet Union and adapted its security system to counter them. Furthermore, these events highlight the extremely important role of border formations in a state's overall national security system.

Keywords: sabotage, Border Protection Corps, diversion

MICHAŁ MYDŁOWSKI*

TECHNOLOGICAL INNOVATIONS AS A CHALLENGE FOR THE UNION AND CONFEDERATE ARMIES DURING THE AMERICAN CIVIL WAR

*Unaffiliated

From the very onset of the American Civil War, commanders, many of whom were trained in Napoleonic-like warfare, faced the unknown reality of modern war. Rapid transportation by railways, long-range firearms and artillery, and the telegraph were just the tip of the iceberg of changes between wars of the past and the Civil War. With these innovations, operational and tactical levels of warfare were profoundly transformed. No longer were armies restricted in their movement by the stamina of soldiers and horses. Orders and information exceeded the speed of couriers.

Faced with this reality, commanders of both sides had to improvise and quickly adapt, or risk being outmanoeuvred and out-generaled by the enemy.

The aim of the papers is to show how commanders tackle new challenges created by the rapid development of technology and how they implement new technological innovations. By discussing most prominent examples – Johnson's troop movement via rail in 1861 or Hooker's attempt to "command-by-wire" during the Chancellorsville Campaign – as well as less famous ones like the rail transfer of Hooker's troops to the west, the paper will depict opportunities and risks of improvised use of technological innovations in warfare.

Keywords: American Civil War, technology, railway, innovations

ETHAN RAFUSE*

WARNINGS UNHEEDED: A TALE OF TWO OFFICERS AND USING THE PAST TO THINK ABOUT THE WARS OF THE FUTURE

*US Army Command and General Staff College

In 1986, Maj. David Petraeus published an essay warning that US Army leaders might be misapplying the lessons of history by using the Vietnam experience to guide their thinking about evolving security threats, defence policy, and battlefield dynamics. Five years later, though, the effort to bring the Army out of its post-Vietnam doldrums by focusing on preparation for large-scale combat operations seemed to receive complete vindication from the rout of the Iraqi Army and liberation of Kuwait. Yet even before the last Kuwaiti oil well fire had been capped, Maj. Daniel Bolger published an article – one in which he, like Petraeus, used historical experience to inform military scientific inquiry – warning that the war the Army had just fought would, in all likelihood, not be the one they would get in the future. Petraeus and Bolger would see their concerns validated in Iraq and Afghanistan. They would also experience mixed results as senior officers in dealing with the problems American arms faced in Iraq and Afghanistan. This presentation will use their earlier writings and the responses to them as a point of departure for considering the challenges military leaders and institutions face as they think about the strategic environment and wars of the future, and illuminate the role of military sciences as a bridge between operational experience and actionable defence innovation.

Keywords: defence policy, strategic adaptation, military history, military education, generalship, future war

VIESTURS RASNACIS*

OPERATIONAL NECESSITY AND INSTITUTIONAL INNOVATION: THE LATVIAN BORDER GUARD IN DEFENCE TRANSFORMATION, 1991–1997

*University of Latvia and Ikšķile Secondary School

This paper examines the formation and development of the Latvian Border Guard between 1991 and 1997 as a case of small-state defence transformation under conditions of institutional scarcity, post-Soviet military legacy, and external security pressure. After the restoration of independence, Latvia had to re-establish effective border control while Russian Federation forces remained on its territory and national defence structures were still being created. In this context, the Border Guard was not merely an administrative border-control service. It functioned as a hybrid military-security institution within the emerging Latvian defence system.

The paper analyses the Border Guard's institutional position in the Defence Forces, its personnel structure, training, supply problems, inherited Soviet infrastructure, discipline issues, and gradual adaptation to Western standards. It also examines the transfer of the Border Guard to the Ministry of the Interior in 1997 as part of the broader specialisation of Latvia's security institutions. The study is based on Latvian Ministry of Defence archival documents, Border Guard archival notes, regional battalion records, oral history interviews, contemporary press, and quantitative data on personnel, conscription, supply, and financing.

By situating the Latvian case within a broader Baltic and post-communist context, the paper argues that border control was a key element of practical sovereignty and defence transformation. The Latvian Border Guard illustrates how operational necessity in a newly restored small state generated institutional innovation, shaped civil-military boundaries, and contributed to the broader reorientation of security institutions toward Western defence and internal security models.

Keywords: Latvia, Latvian Border Guard, 1990-s transformation, security, defence

RAFAIL REKOUNIOTIS*

THE RETURN OF TERRESTRIAL REALITY: LESSONS FROM INTERWAR GEOPOLITICAL CHOKEPOINTS

*University of Athens

Despite the contemporary pivot toward multi-domain operations and network-centric warfare, the fundamental constraints of physical geography have reasserted themselves as the primary variables of European security. This paper will examine the enduring strategic relevance of Northern European terrain, tracing how the chokepoints and logistical corridors that defined the interwar security calculus continue to dictate modern military posture. By analyzing historical defense strategies against the demands of current hybrid and multi-domain environments, the paper will demonstrate that the requirements for “strategic depth” have remained remarkably consistent over the last century.

The paper will argue that the modern digital-first approach to security often obscures the persistent and sometimes challenging physical reality of the European theater of operations. By bridging historical scholarship and contemporary operational analysis, the paper aims to provide a critical lens on current military planning, suggesting that the drive for technological integration must be balanced by a renewed mastery of physical geography. The paper will conclude by offering a historical critique of modern security assumptions, asserting that geographical control remains the essential, yet often neglected, foundation of military capability and regional resilience.

Keywords: strategic geography, interwar diplomacy, chokepoints, strategic depth

JEAN-PIERRE SCHERMAN*

'PEACEKEEPING OPERATIONS IN THE DRC ARE NOT PEACEFUL' THE SOUTH AFRICAN NATIONAL DEFENCE FORCE BATTLES AGAINST THE M-23 REBEL GROUP

* Stellenbosch University, Faculty of Military Science

On 05 April 2001, the first 88 soldiers of the South African National Defence Force Specialist Contingent (SANDFSPECC) left South Africa bound for the Democratic Republic of the Congo (DRC) as members of MONUC. This involvement by the SANDF in UN Peace Keeping Operations (PKO) was to be the first ever undertaken by the country. From such humble beginnings, the SANDF commitment to the DRC was to expand significantly so that by the time that MONUC was replaced by a new MONUSCO on 01 July 2010, SA's troop strength was approximately 1,200 soldiers divided amongst UN Staff Officers, SANDFSPECC personnel, and combat personnel in the form of an infantry battalion group supported by a composite helicopter unit.

The transition from MONUC to MONUSCO was to bring the SANDF into direct contact with the M-23 Rebel Group. Beginning with M-23's conquest of the capital city of Goma, North Kivu Province, in November 2012, South African soldiers would find themselves on the front lines of a clash that was to eventually involve the offensive deployment of South African special forces snipers, APCs, and even South African attack helicopters. Whilst the 2012-2013 fighting inflicted heavy casualties on M-23 it did not eliminate their presence from the eastern DRC. Sporadic fighting would continue between the two groups for the next thirteen years with the body count continuing to grow on both sides. It would eventually culminate in another fierce round of fighting in January 2025, which would cost the lives of another 15 South Africans and bring the SA total death count to over 100 peacekeepers killed. This continued loss of life in not-so-peaceful PKOs within the DRC would prompt the South African government to withdraw the SANDF from the DRC after a deployment of a quarter century – the longest ever by the South African armed forces. This paper will examine this deployment for the first time, which is still classified by the SANDF, using currently available open sources.

Keywords: South African National Defence Force, Democratic Republic of Congo, MONUSCO, M-23 Rebel Group, Goma, North Kivu

EVANDRO SOARES*

PEACE OPERATIONS AND THE HISTORICAL TRANSFORMATION OF INTELLIGENCE AFTER THE COLD WAR: ONUCI AND THE EVOLUTION OF MULTINATIONAL INFORMATION PRACTICES

*Universidade Presbiteriana Mackenzie (UPM, Mackenzie Presbyterian University)

Peace operations are frequently examined through diplomatic, humanitarian, or legal perspectives, but remain comparatively understudied as historical spaces of military adaptation. This article argues that United Nations peace operations after the Cold War served as laboratories for the evolution of multinational intelligence practices amid fragmented sovereignty, hybrid conflict, and informational uncertainty.

The collapse of bipolarity challenged conventional military doctrines inherited from the Cold War. Intrastate conflicts, irregular armed actors, and transnational networks required informational capabilities extending beyond traditional state-centred military intelligence. The article examines this transformation through the United Nations Operation in Côte d'Ivoire (ONUCI), particularly during 2005–2006, and interprets the mission as part of a broader historical transition that affects the relationship among warfare, governance, and information management.

The paper adopts a historical-institutional approach at the intersection of military history, intelligence history, and operational adaptation, drawing on Kaldor, Van Creveld, Strachan, and Heuser, and on UN doctrinal reforms following the Brahimi Report.

Three arguments are sustained: post-Cold War peace operations accelerated the institutional normalisation of multinational intelligence-sharing; missions such as ONUCI integrated HUMINT and open-source environments before the consolidation of contemporary digital intelligence systems; and peace operations anticipated informational dynamics later associated with hybrid warfare.

The study concludes that peace operations should be understood not only as instruments of international stabilisation, but as historically significant environments in which the informational logics of twenty-first-century conflict were first operationally tested.

Keywords: peace operations, multinational intelligence, ONUCI, post-Cold War warfare, hybrid conflict, military adaptation, Brahimi Report, HUMINT

JACOB THOMAS-LLEWELLYN*

OLD HISTORY – NEW AUDIENCE: THE INFLUENCE OF THE MULBERRY HARBOURS ON CONTEMPORARY CHINESE PREFABRICATED INVASION PLATFORMS

*Rabdan Academy

It has been almost 90 years since the Allied powers landed on the beaches of North-West Europe on 6th June 1944, but the influence of this operation is still being felt today in the realm of military civil engineering. The planners for the largest amphibious invasion in history, Operation OVERLORD, were forced to recognise that in order to establish a bridgehead on the enemy shore, they would need a well-founded port to support their logistical build-up. The solution was to design, fabricate and deliver two mobile harbours, each weighing over one million tons, across the English Channel.

In the 21st Century, China is facing the same conundrum as the Allied planners in 1944. The Chinese military has been contemplating how they might execute and sustain an amphibious invasion of Taiwan, and the answer lies with studying Project MULBERRY. It is now well established that China has completed prefabricated pierheads based upon elements of the MULBERRY Harbours and is looking to emulate additional designs and components. The aim of this paper is to demonstrate how historical examples of military engineering can influence future planning and provide key insights, especially in the realm of military logistics and defence industry expansion during a time of national emergency.

Keywords: amphibious, engineering, OVERLORD, China

JACOB THOMAS-LLEWELLYN*

FUEL IN THE DEEP: THE PLANNING AND OPERATIONAL LESSONS OF PROJECT PLUTO, 1943-1945

*Rabdan Academy

The Pipeline Under the Ocean (PLUTO) was a secret government project devised in the close of 1942. The intention was to lay a fuel pipeline across the English Channel in order to support the invasion of Northwest Europe. The project encountered significant challenges at the design, fabrication and operational stages. Using a combination of rare and previously closed archival sources, this paper will shed light on one of the most complex and high-risk projects of the Second World War to provide valuable lessons for present and future practitioners.

Keywords: PLUTO, design, fabrication, operational

TIAGO ABRÃO VILINGA*

THE ROLE OF UN MISSIONS IN PEACEBUILDING IN ANGOLA (1989-1997)

*Brazilian Army Command and General-Staff College (ECEME)

This article analyzes the role of the United Nations (UN) in managing and resolving the Angolan civil war through the verification missions UNAVEM I, II, and III, covering the period from 1989 to 1997. Contextualized within the Cold War framework, the research examines how the rivalry between MPLA and UNITA escalated into a proxy conflict fueled by external powers. Using a descriptive-analytical approach, the study breaks down the specific mandates of each mission to evaluate their outcomes. UNAVEM I successfully supervised the withdrawal of foreign troops from Cuba and South Africa. UNAVEM II, established after the Bicesse Accords to oversee the 1992 democratic elections, failed to maintain peace when the electoral results were rejected, leading to a resurgence of violence. Finally, UNAVEM III, anchored in the Lusaka Protocol, demonstrated the importance of robust mandates and diplomatic persistence in achieving fighter demobilization and disarmament. Additionally, the paper highlights the relevance of multilateral diplomacy and Brazil's significant contribution to these peace operations, particularly in UNAVEM I. The Angolan experience serves as a key case study, reaffirming that international cooperation and dedicated diplomacy remain fundamental pillars for rebuilding stability in nations torn by internal conflicts.

Keywords: UN, UNAVEM, Angola, peacekeeping operations, multilateral diplomacy, civil war

ADRIAN WETTSTEIN*

'ALMOST ALL OF THE MEN ARE APATHETIC TO THE POINT THAT THEY COULD NOT CARE LESS WHETHER THEY ARE SHOT DEAD BY THEIR OWN OFFICERS OR BY THE RUSSIAN': THE GERMAN 'INFANTRY CRISIS' IN 1943/44.

*MILAK

With the outbreak of the German-Soviet War in the summer of 1941, the nature of warfare fundamentally changed for the German Army. Not only were losses now higher than they had been in other theatres, but they occurred month after month, and so did material losses and consumption of goods. Before long, the German army found itself mired in precisely the war of attrition it had sought to avoid. Furthermore, the kind of war most of the German army fought from late 1941 onwards was mainly a positional and defensive one, entirely different from the offensive mobile warfare it had become accustomed to and demanding a shift in doctrine, training and leadership. The German Army's efforts to adapt to these challenges, while executed swiftly and with determination, lacked efficiency overall. This, and the immense Soviet superiority in men and material caused German fighting power to erode steadily over the course of the next two years. The situation culminated in the summer of 1943, when a significant number of infantry units saw most of their fighting power whittled away through a mixture of excessive deployment, sheer exhaustion, insufficient replacements (both in number and quality), a lack of material and modern weaponry and, finally, persistent underappreciation within the armed forces and society as a whole. As these units comprised the bulk of German combat troops, their plight was cause for alarm among military leadership and the German Army's central institutions, who labeled the situation an "Infantry Crisis". Based on original research of German files, this paper will contemplate the reasons for the "Infantry Crisis", its perception, proposed solutions and finally the measures taken to remediate its worst effects.

Keywords: World War II, Wehrmacht, German-Soviet War, infantry

WORKING GROUP 3:
MILITARY TECHNOLOGY

Chair

CHRISTOPHER RENAHAN
Royal Military College of Canada

Co-Chair

DRUVIS KLEINS
Baltic Defence College

OYKU CAGLAYAN*
ALEKSANDRS STUPENKOVS[2], VIKTORS GUTAKOVSKIS[3], UGUR GOLAL[4]
DEVELOPMENT OF A HIGH-EFFICIENT BATTERY PACK FOR THE UAV

*-[4]Riga Technical University

Unmanned Aerial Vehicles (UAVs) are increasingly deployed across surveillance, logistics, agriculture, and defense applications, where flight endurance, payload capacity, and operational reliability are critical performance factors. The battery pack is a key limiting component, directly influencing mission duration, energy efficiency, and safety. This study presents the development of a high-efficiency battery pack optimized for UAV applications, focusing on maximizing energy density while ensuring thermal stability, electrical reliability, and operational safety.

The proposed battery pack design integrates advanced optimized cell configuration and lightweight structural materials to achieve improved gravimetric and volumetric energy density. A smart Battery Management System (BMS) is developed to enable real-time monitoring of voltage, current, temperature, and state of charge, while providing active balancing and fault protection. Thermal management strategies, including passive heat dissipation and airflow-assisted cooling, are incorporated to maintain optimal operating conditions during high-power flight phases.

Performance evaluation demonstrates enhanced discharge efficiency, extended flight time, and reduced energy loss under dynamic load profiles typical of UAV missions. Safety mechanisms addressing overcharge, over-discharge, and thermal runaway risks are validated through laboratory testing. The results indicate that the developed high-efficiency battery pack significantly improves UAV endurance and reliability, offering a scalable and adaptable solution for next-generation UAV platforms.

Keywords: UAV, battery, FPV, smart Battery Management System

ABDELLAH CHEHRI*

PROTECTING DRONES: SMARTER SECURITY FOR A CONNECTED SKY

*Royal Military College of Canada

Unmanned aerial vehicles (UAVs) are increasingly deployed in mission-critical applications such as emergency response, environmental monitoring, precision agriculture, and defense operations. As UAV adoption accelerates, the risk of signal spoofing, interference, and unauthorized control continues to grow. Traditional software-based protections – such as passwords, encryption, and access codes – provide important layers of defense but remain vulnerable in dynamic and adversarial wireless environments. A promising complementary direction is physical-layer authentication, which leverages the unique radiofrequency (RF) characteristics produced by each UAV controller.

Every UAV controller has tiny hardware imperfections that create a unique "signature" in its radio signal – similar to a fingerprint. By learning these patterns, it becomes possible to determine whether a signal truly originates from the legitimate controller or from an attacker attempting to impersonate it. This work introduces an adaptive RF-based identification framework that enhances UAV communication security by combining physical-layer signatures with artificial intelligence. By using AI, the system can effectively "listen" to a UAV's signal and determine whether it comes from an approved controller or from a malicious source attempting to cause disruption. This strengthens authentication by relying on intrinsic signal features that are extremely difficult to forge or manipulate. A key contribution of this work is its ability to adapt as new UAVs are added to the network. UAV fleets evolve over time as new models are introduced and older devices are retired. To address this, the framework incorporates a continual learning mechanism that enables the system to integrate new UAVs without needing to start from scratch or retrain the entire model. This ensures long-term scalability while preserving knowledge of previously learned devices.

Keywords: drones, UAV security, smart authentication, artificial intelligence, safer skies

JARBAS ALFEU DE PAULA JUNIOR*
EDUARDO XAVIER FERREIRA GLASER MIGON[2]

QUANTUM SENSING, MILITARY EFFECTIVENESS, AND THE FUTURE TRANSPARENCY OF THE BATTLEFIELD

*-[2]Military Engineering Institute and Brazilian Army Command and General Staff College (ECEME)

Quantum technologies are increasingly framed as disruptive enablers of future military capability, yet their most plausible near-term impact is unlikely to emerge from general-purpose quantum computing. This paper argues that quantum sensing represents the most operationally relevant pathway through which quantum technologies may affect military effectiveness in the next decade. Rather than treating quantum technology as a single revolutionary package, the paper distinguishes between sensing, communications, and computing, and examines their different levels of technological maturity, operational feasibility, and doctrinal relevance. The central argument is that quantum-enabled military advantage is likely to emerge first as an advantage in perception, positioning, navigation, timing, and synchronization. Quantum sensors may improve resilience in GPS-denied environments, enhance measurement of magnetic, gravitational, inertial, and temporal variables, and support operations in increasingly contested multi-domain battlespaces. However, the paper rejects deterministic claims that quantum sensing will automatically nullify stealth, submarine concealment, or existing operational doctrines. Instead, it proposes the concept of gradual transparency pressure: a cumulative erosion of concealment advantages produced by more sensitive, distributed, and multi-domain sensing architectures. Methodologically, the paper adopts a strategic and doctrinal assessment of emerging military technology, combining literature on quantum military applications, defence innovation, and future warfare. It evaluates quantum sensing through three analytical dimensions: operational effect, integration constraint, and doctrinal consequence. The analysis suggests that the key problem is not only technological maturity, but the ability of armed forces to cross the implementation “valley of death” between laboratory demonstrations and deployable military systems. The paper contributes to debates on military technology by shifting attention from quantum hype to capability translation. It concludes that quantum sensing should be understood less as a stand-alone weapon of disruption and more as a driver of resilient command, distributed operations, and changing relations between detection, concealment, and decision advantage.

Keywords: quantum sensing, military effectiveness, GPS-denied environments, multi-domain operations, decision advantage

NATHAN ESKUE*

THE CONVERGENCE OF EVOLVING THREATS, AI CAPABILITY, AND NEXT-GEN COMPUTING WILL CHANGE THE BATTLEFIELD

*Planck Dynamics and TU Delft Aerospace Engineering

Recent conflicts in Ukraine and the Middle East have provided a stark reminder that warfare will always be at the cutting edge of technology adoption. Drone warfare has been a prominent indicator of radical tactic evolutions. However, this is just part of a larger movement that requires us to examine everything from individual tactics to long-term geopolitical decisions. This talk will analyze three key factors driving this change and provide recommendations on how we should address them. Evolving threats such as drones, quantum computing, and digitally connected infrastructure mean that large-scale conflicts will not just happen on the front lines but in all cities. AI capability is changing both offensive and defensive tactics, pointing toward an AI-driven arms/tactics race. Next-Gen computing provides operators in the field the potential for more analytics power than current FOBs. For each factor, we will briefly discuss the current state of the art and what to expect in 3-5 years; how we need to adjust current doctrine to prepare defensive measures for these asymmetric changes; and what actions should be taken now to take full advantage of these rapidly evolving elements that are already changing the face of warfare.

Keywords: AI, Edge computing, quantum computing

VIKTORS GUTAKOVSKIS*
ARTIS IESMINS[2], MEHMET-EFE ILHAN[3]

MODULAR STEEL PAYLOAD MUNITION FOR EUROPEAN FPV/UAV PLATFORMS

*Riga Technical University, [2]Riga Technical College, [3]RTU BMF Institute of Mechanical Engineering

The rapid evolution of First-Person View (FPV) and Unmanned Aerial Vehicle (UAV) platforms in Europe has created demand for standardized, adaptable, and interoperable payload solutions. This study presents the development of a modular DN50 steel payload munition designed to be compatible with a wide range of European FPV and UAV platforms. The objective is to deliver a robust, scalable, and mission-configurable payload architecture while maintaining strict constraints on mass, balance, and aerodynamic efficiency.

The proposed munition utilizes a DN50 steel body as a standardized structural core, enabling modular integration of different functional elements such as fragmentation sleeves, shaped charges, or inert payloads for training and testing. A modular interface system allows rapid assembly, disassembly, and reconfiguration without platform-specific redesign. Emphasis is placed on structural integrity, predictable center-of-gravity alignment, and mechanical compatibility with common UAV mounting systems.

Design optimization includes material selection, wall thickness tuning, and finite element analysis to ensure resistance to launch, transport, and impact stresses. Safety considerations such as secure arming mechanisms, transport-safe configurations, and compliance with European handling standards are incorporated. The resulting system provides a flexible payload solution that enhances operational versatility while reducing logistical complexity. This modular DN50 munition framework supports both operational and developmental use cases and contributes to the standardization of payload architectures for European FPV and UAV ecosystems.

Keywords: UAV, FPV, ammunition, payload, modular

MIKE HARTNETT*
TOM NUGENT[2]

WIRELESS POWER BEAMING AND A NEW MARITIME DOMAIN AWARENESS CAPABILITY

*-[2]PowerLight Technologies

Persistent maritime domain awareness is increasingly critical across the Baltic Sea for securing commercial infrastructure and national security. Aerial unmanned autonomous systems (UAS) provide intermittent Intelligence, Surveillance, and Reconnaissance (ISR) coverage, but long-endurance, larger platforms are expensive and therefore limited, while smaller, more cost-effective UAS are constrained by batteries, limiting flight endurance. Both challenges result in intelligence gaps when UAS must break coverage to land for refuelling and battery swaps, thus increasing the risk of malign activities or surreptitious attacks happening in and across the Baltic Sea.

Recent advances in wireless power beaming, demonstrated by PowerLight Technologies at Shaw Air Force Base, in the US, now enable dynamic power distribution to UAS aloft, extending their range, operational endurance, and payload capacity.

Employed in support of persistent ISR operations, this new capability enables the creation of a continuous maritime sensing architecture across the Baltic that would generate new longitudinal patterns of life data sets to distinguish normal commercial maritime activities from coordinated adversarial manoeuvres and “grey-zone” activities meant to deter, disrupt, or even target lawful commercial and naval activities across the Baltic.

This abstract proposes to provide a briefing on the PTROL UAS programme, present data, results, and new modelling tools from the Shaw AFB demonstrations, and discuss how this new capability could be employed by Nordic and Baltic states to enable a new, more persistent, and cost-effective maritime domain awareness capability for allies and partners across the Baltic Sea.

Keywords: border, awareness, autonomy

TAL INBAR*

THE ULTIMATE CHALLENGE: STRATEGIC, OPERATIONAL, AND TECHICAL LESSONS FROM IRAN'S MISSILE WARFARE

*Missile Defense Advocacy Alliance

This paper examines the operational lessons drawn from Israel's two recent confrontations with Iran – Operation Rising Lion (June 2025) and Operation Roaring Lion (also known as "Epic Fury", beginning February 2026) – as the most demanding real-world trials yet faced by integrated missile defense architectures. Drawing on official IDF disclosures, defense-establishment assessments, and open-source reporting, the analysis traces how Iran's ballistic missile and UAV doctrine evolved between the two campaigns: from the massed, synchronized salvos of dozens of missiles in Rising Lion to a deliberate "drip-feed" tactic in Roaring Lion.

The paper assesses how Israeli and American air and missile defense layers adapted in real time. It further considers the strategic tension between interdicting launch capability at the source (strikes on production, storage, and tunnel infrastructure) versus relying on terminal defense, arguing that the qualitative shift in Iranian launch doctrine – from overwhelming numbers to sustained, low-volume harassment, represents an emerging asymmetric response to layered defense systems.

The paper concludes with policy implications for force planning, interceptor stockpile management, and coalition coordination, emphasizing that missile defense success must be measured not only by intercept percentages but by sustainability under prolonged, multi-front pressure. These operational and strategic lessons are highly relevant to other theatres outside the Middle East.

Keywords: missile defense, Iran, ballistic missiles

MD MUHIDUL ISLAM KHAN*

INTELLIGENT SPECTRUM MANAGEMENT FOR DEFENCE: LEVERAGING AI-DRIVEN 6G COMMUNICATION ARCHITECTURES IN MULTI-DOMAIN MILITARY OPERATIONS

*Norwegian Armed Forces

Recent conflicts have made clear that control of the electromagnetic spectrum is no longer a supporting function in modern warfare; it is a core operational capability. As armed forces operate across land, sea, air, space, and cyberspace simultaneously, the demand for resilient, adaptive communications has grown sharply, and existing infrastructure is struggling to keep pace. Sixth-generation (6G) wireless technology offers a credible path forward. With terahertz-band throughput, sub-millisecond latency, and AI-native architecture, 6G is not simply an upgrade on what came before. It opens new possibilities for how military networks are designed and managed, though it also introduces new vulnerabilities in contested environments where jamming, spoofing, and cyber-electronic attack are routine. This paper proposes a framework for AI-driven spectrum management tailored to defence-grade 6G deployments. Drawing on deep reinforcement learning and federated learning, the approach enables dynamic frequency allocation, real-time interference mitigation, and sustained connectivity under degraded conditions. Generative models are also explored for anomaly detection at the tactical edge, where cloud-dependent solutions are too slow to be useful. The findings are simulation-based, but the questions behind them come from operational experience. The goal is not to offer a finished solution, but to advance the conversation about how military communications must evolve as the electromagnetic battlespace grows more contested, and how the lessons of current conflicts should inform the systems we build next.

Keywords: 6G communications, artificial intelligence, machine learning, spectrum management, multi-domain operations, electronic warfare, tactical edge computing

SUZANA LAMPREIA*
VALTER VAIRINHOS[2], VICTOR LOBO[3]

DYNAMIC MAINTENANCE ON SHIPS WITH PYTHON

*-[3]Portuguese Naval Academy

Dynamic maintenance on ships has been significantly enhanced through the integration of data-driven approaches and modern programming tools such as Python. In the past, ship maintenance relied on preventive and corrective maintenance, where scheduled inspections and corrective actions were taken, respectively, to prevent and correct a failure on a system or equipment. However, this approach often led to increased operational costs and unavailable equipment for a longer time. Dynamic maintenance, supported by Python, enables a shift toward predictive and condition-based strategies. Python provides an adaptive system for data analysis, machine learning, and system modeling, making it particularly suitable for maritime applications. Collecting data from ship sensors such as temperature, vibration, and pressure allows technicians to continuously monitor the health of critical and selected systems. Python based language-software may allow identify patterns and anomalies, supporting early fault detection and prognosis. Combining the Failure Mode, Effect, and Critically Analysis (FMECA) with real-time data enhances the prioritization of maintenance tasks dynamically, rather than relying on static risk assessments. Python may integrate with an existing ship maintenance management system, facilitating automated alerts and decision support systems. This concept may contribute to safer operations, optimized resource allocation, and extended equipment life.

Keywords: maintenance, ship, dynamic, Python

MARCEL MANGOLD*

SHIFTING SOCIO-TECHNICAL PARADIGM: THE CASE OF SWEDISH UAV CAPABILITY BUILD-UP

*Swedish Defence University

This project examines the large-scale build-up of Swedish Unmanned Aerial Vehicle (UAV) capability since the end of 2024. Like many other states, based on lessons from Ukraine, Sweden has identified the need to rapidly build a large-scale UAV capability, including developing conditions to sustain the mass of such capabilities and their renewal over time. These efforts, however, face several challenges: compared to Ukraine and Russia, which are at war, countries officially not at war have difficulty adapting to the rapid changes in this new form of warfare and the systems, dual-use technologies, and procurement models that have emerged with it. Building on interviews with military officials and other participants in Sweden's efforts to build UAV warfare capability, this presentation explores how this challenge has been understood and addressed. Three levels in this process are traced: how problems have been formulated and addressed; how actors create organizational innovations that remove obstacles and enable adaptation; and, finally, a conceptualization of the new socio-technical assemblages of adaptation that have emerged and what remaining problems they face. Drawing on theories of military adaptation, the analysis focuses on how new practices, strategic concepts, and doctrines are developed to enable adaptation in this context, and how techniques, tactics, and procedures are redefined by central actors in this process. The focus is also on emerging institutions, infrastructure, new forms of procurement, training, and exercises, as well as shocks to existing practices and norms. The results are discussed in relation to scholarship on cultural factors in military organization and military adaptation, literature on socio-technical change, and other case studies of how UAV warfare capability has been adapted elsewhere.

Keywords: socio-technical assemblages, UAV warfare, Swedish Armed Forces, military adaptation, civil-military relations

JUHA MATTILA*

CYBER AND ELECTROMAGNETIC ACTIVITIES (CEMA) IN A MULTI-DOMAIN BATTLEFIELD

*Aalto University

Contemporary adversaries aim to integrate lines of operations across information, cyber, electromagnetic, and kinetic domains. They take advantage of the digitalisation of the information landscape, which opens avenues to deliver impact at the cognitive and social levels.

Simultaneously, the demand for mobility and dispersion on the battlefield multiplies the need for transceivers and wireless communication. Naturally, this increases the targets for electronic attacks. The military is gradually integrating cyber and electromagnetic capabilities into its portfolio, but often lacks appreciation of their combined impact on a modern multi-domain battlefield. The research uses design science methods to develop a model of Cyber-Electromagnetic Activities (CEMA) and Enterprise Architecture (EA) views, illustrating them in the context of a modern multidomain battlefield. Firstly, research defines modern Cyber-Electromagnetic battlespace and derives its tenets from real-world cases. Secondly, research elaborates on the combined CEMA in the context of multidomain operations. Thirdly, research designs a CEMA model, illustrates it using views typical of enterprise architecture, and finally tests the model's feasibility. The findings of this research provide insights and explanations to planners and researchers of operational art that: CEMA is always a part of multi-domain operations because of its omnipresence, CEMA, being a composition of many abilities, needs collaborative planning and orchestration of execution, both in defensive and offensive operations, asymmetric operational thinking opens a spectrum of means and ways to effect in a multidomain battlefield, rapidly evolving technology opens both vulnerabilities and avenues of effect for defensive and offensive operations, and advanced digital force will dominate a force with commercial or dual-use technologies in modern multi-domain operations.

Keywords: cyber operations, electronic warfare, CEMA, multi-domain operations, design sciences

ANA MOITA*
TOMAS CALAPEZ[2], PEDRO PONTES[3], JOAO TORRES[4]

MICROCHANNEL BASED HEAT SINK FOR THE THERMAL MANAGEMENT IN UAVS: EFFECT OF TILT ANGLE UNDER STEADY STATE AND TRANSIENT CONDITIONS

*,[3]IST-University of Lisbon, [2]IST-University of Lisbon/CINAMIL - Portuguese Military Academy, [4]CINAMIL - Portuguese Military Academy

Unmanned Aerial Vehicles (UAVs) play a major role in various military and emergency operations, from surveillance and reconnaissance to striking missions. The performance of the electronic systems is paramount in the success of the UAV's performance, for which efficient thermal management systems are an increasingly important factor. In this context, this paper presents a work in progress following a project involving the University of Lisbon and the Portuguese Army to develop and test a thermal management system based on a passive microchannel heat sink designed to cool the avionics of an unmanned aerial vehicle (UAV), which is used by the Portuguese Air Force. The proposed system exploits the phase-change properties of a dielectric fluid to enhance heat removal through latent heat of vaporization, as phase-change at ambient temperature occurs at the relevant working temperature of the electronic components (approximately 61ºC). The low relative importance of gravitational forces in microchannel flows enables the system to operate under diverse dynamic conditions. Following prior work in which basic heat sinks were developed and tested under steady-state and transient conditions, this work now tests benchmark power dissipation curves representative of real flight conditions. The performance of the heat sink is evaluated regarding heat flux removed, heat transfer coefficients, pressure drop and power pump requirements for different orientations and tilt angles of the heat sink. Results show that the optimized channel geometry with curved and divergent channels plays a decisive role in thermal system being able to cope with the required thermal power dissipation requirements both in steady-state (cruise flight) and transient (take off) conditions.

Keywords: heat sink, microchannel, two-phase flows, tilt angle, UAV

VLAD ONEȚIU*

FROM EARTHQUAKE ALERTS AND AI INTELLIGENCE TO MULTI-DOMAIN DEFENCE

*CYBOV

Sudden, large-scale threats – whether natural or adversarial – share a common operational structure: a detection event, a narrow window to warn exposed assets, and a critical period in which commanders must build situational awareness from distributed, incomplete sources. A missile or drone incursion, a hybrid attack on critical infrastructure, and a major earthquake differ in cause but impose the same coordination problem. This paper presents a threat-agnostic system backbone for that problem, and demonstrates it on earthquakes as a live, low-risk proving ground.

The backbone follows a *detect-alert-coordinate* pipeline and embodies an architectural thesis we term *decoupling speed from intelligence*. A detection signal – today a national seismic feed, tomorrow a radar, sensor, or early-warning input – triggers two deliberately separated paths. A fast, dependency-minimal alerting path warns exposed institutions within seconds, segmenting recipients by time-to-impact rather than geography. A slower, AI-assisted intelligence layer then closes the commander's information gap: it queries affected institutions in parallel, parses free-text responses into structured status, correlates external open-source signals, and presents a synthesised, access-controlled picture that mirrors command hierarchy – rather than a flood of raw reports.

We argue this separation is the key to resilience under disruption: the alerting path never depends on the heavier intelligence processing, so warnings survive even when synthesis degrades. We detail the event-driven, cloud-native design that delivers this at low cost, contrast it with a documented national crisis-system failure built on heavy centralised infrastructure, and show how the same backbone generalises from seismic events to missile, drone, and hybrid-threat scenarios. We close with the implications for NATO interoperability and dual-use defence innovation: a coordination layer proven in civil protection today, transferable to multi-domain threat response tomorrow.

Keywords: dual-use technology, crisis response, resilience, command and control, situational awareness

JUUSO PELTTARI*
TUOMAS JALONEN[2], EETU JÄRVI[3], JONI KENTALA[4], JARKKO MARIN[5], JAN MIETTINEN[6], JERE HEIKKINEN[7], TUOMAS MÄKINEN[8], HENRI LAMMINAHO[9]

FROM ARMOR TO MIND: BALLISTIC PROTECTION AND COGNITIVE RESILIENCE AGAINST IEDS AND DRONE WARFARE

*-[9]Finnish National Defence University

This study evaluates the significance of vehicle ballistic protection for cognitive performance and subjective safety under asymmetric threats. Analyzing a December 2025 field test of vehicle-mounted armor against fragmentation from hand grenades to 120 mm mortar shells, this paper integrates empirical data with literature on blast physiology, drone warfare's psychological burden, and cognitive resilience to examine how technical protection and soldier well-being interlink under extreme stress.

IED exposure and constant UAV presence induce psychological burdens and hypervigilance regardless of direct contact (Freh et al. 2013). Blast mTBIs strongly link to PTSD – with 43.9% meeting criteria (Hoge et al. 2008) – and CTE risks (Goldstein et al. 2012). Drone sounds and strike videos amplify this fear (Bonvie et al., 2025). Mitigating these threats requires physical shields, realistic training, and electronic warfare, especially against fiber-optic drones (Tytarenko et al. 2025).

The field test proved that the vehicle-mounted armor provides exceptional fragmentation shielding against all explosives used. Synthesizing these physical outcomes with psychological frameworks shows that validated technical protection acts as an immediate psychological buffer. Restoring a soldier's sense of control under fire transforms tactical terror into a manageable professional risk rather than cognitive paralysis (Norris et al. 2015).

Novelly, this paper bridges tactical engineering and cognitive resource management. While traditionally studied in isolation, this study demonstrates that technical survivability acts directly as a cognitive multiplier. The paper advances military literature by showing how physical defensive countermeasures systematically lower mental workload, thereby preserving personnel's critical decision-making capacity under fire. This integration provides planners a holistic readiness framework, shifting focus from material endurance to total socio-technical resilience.

Keywords: ballistic protection, drone warfare, cognitive resilience, combat effect, psychological buffer

DANIELE SEGRETO*

PRE-ENERGIZED LAUNCH ARCHITECTURES FOR ATTRITION-BASED COUNTERUAS DEFENCE SYSTEMS

*Università degli Studi di Palermo

Recent conflicts demonstrate how the proliferation of low-cost unmanned aerial systems (UAS) and loitering munitions is reshaping the cost-exchange balance of contemporary air defence**.** Contemporary battlefields – from Nagorno-Karabakh to Ukraine – reveal that low-cost drones (USD 400-1,500) now account for 62-70% of equipment losses, establishing unprecedented cost ratios up to 1:25,000 that render traditional interceptors economically unsustainable. As autonomous navigation and onboard intelligence reduce the effectiveness of traditional electronic warfare, defence systems must translate operational insights into scalable capability transformation.

This paper proposes a conceptual framework for an attrition-oriented, low-logistical-footprint point-defence architecture that integrates passive detection, mechanically pre-energized launch systems, and radio-independent autonomous terminal guidance enabled by edge AI and onboard computer vision. Recent advances in YOLOv8-based real-time object detection (93% accuracy) and lightweight edge processors demonstrate technical feasibility for autonomous guidance in contested electromagnetic environments without reliance on GPS or external communication links.

The framework's novelty lies in unifying mechanical pre-acceleration, autonomous visual engagement, and cost-exchange modelling within a coherent defensive paradigm. Three analytical dimensions structure the assessment: engagement latency reduction through pre-energized architectures; resilience under electronic attack via vision-independent terminal guidance; and recalibration of cost-exchange dynamics through simplified, expendable interceptors. By integrating operational experience with emerging AI technologies and cost-effectiveness principles, the study contributes to military science and defence transformation doctrine in the era of mass-drone warfare.

Keywords: counter-UAS, attrition warfare, cost-exchange ratio, passive defence architecture, Edge AI, guidance systems

GUNTIS SKUNSTINS*

THE CHANGING FACE OF THE BALTIC DEFENSE INNOVATION ECOSYSTEM

*University of Latvia

The fear of war in Europe has drawn attention to technological innovation and development to enhance national defense forces and secure strategic war materiel for these forces, whether on land, at sea, or in the air, to defend the nation and secure independence. The concern of strategic supply chain security, development of indigenous defense innovation, and the industry's ability to close the capability gap between small armed forces and dominant adversary, and to provide national armed forces with the newest technologies, has pushed the Baltic States governments to adopt strategies, stimulating innovation and growth of the thereby connected defense sector ecosystem. And while unmanned aerial drones and counter-UAV technologies have gained undivided attention, the development of naval capabilities has remained in the shadows, with its own specific issues and challenges. While using publicly available data from Estonia, Latvia, and Lithuania and conducting interviews with defense experts, the research focused on naval technological innovation and industry in 3Bs, indicating that the Russian invasion of Ukraine has accelerated the Baltic development of the defense innovation ecosystem for naval warfare as well; however, the capability and capacity of this specific defense industry branch are limited to date.

Keywords: navy, defense, industry, ecosystem

ZI YANG*

THE RUSSIA–UKRAINE WAR AND CHINA'S AI-DRIVEN MILITARY MODERNIZATION

*S. Rajaratnam School of International Studies

The Russia-Ukraine War represents the most significant conventional warfare of the 21st century. As the conflict enters its fourth year, it has evolved into a critical laboratory for "intelligentized" military equipment, novel tactical applications, and modern operational concepts. This paper examines how Chinese military researchers have conducted exhaustive analyses of this conflict, interpreting it not merely as a localized struggle between neighboring states, but as a high-stakes confrontation between Russia and the US-led Western Bloc – a coalition China views as its primary potential wartime adversary. Drawing from an extensive review of Chinese military literature and strategic discourse, this study asserts that the People's Liberation Army is actively integrating observed lessons from the Ukrainian theater into its military modernization initiatives and contingency planning. The research identifies four primary areas of focus in China's critical assessment: the enhancement of joint operations command-and-control systems, the transformative role of unmanned systems, the decisive impact of electronic warfare, and the complexities of modern wartime logistics. Ultimately, this paper argues that the Russia-Ukraine War is fundamentally reshaping China's evolving doctrine of "intelligentized warfare".

Keywords: Russia-Ukraine War, China, artificial intelligence, military reform, intelligentized warfare

KACPER ZDROJEWSKI*

ARCHITECTING THE AUTONOMOUS BATTLEFIELD: SYNERGIZING AI DISTRIBUTED CONNECTIVITY, AND THE EVOLUTION OF HUMAN CONTROL

*War Studies University in Warsaw, Regional IT Center Warsaw

The contemporary battlefield is undergoing a paradigm shift driven by the rapid convergence of advanced communications, artificial intelligence (AI), and autonomous systems. Aligned with the theme of defence innovation, this presentation explores the synergetic integration of these emerging technologies and their transformative impact on military operations and command-and-control (C2) architectures. Firstly, the research examines the critical requirement for resilient, high-bandwidth networking in contested environments. It highlights the integration of commercial proliferated Low Earth Orbit (pLEO) satellite constellations, such as Starlink, with Software-Defined Wide Area Networking (SD-WAN) to ensure uninterrupted, decentralized connectivity and agile traffic routing under heavy electronic warfare constraints. Building upon this robust communication backbone, the study analyzes the implementation of AI as a crucial force multiplier. AI's utility is evaluated not only in real-time battlefield data processing but also in advanced military simulations and wargaming. These virtual environments are essential for developing novel operational doctrines, predictive modeling, and safely testing system resilience before physical deployment. Furthermore, the presentation addresses the accelerated deployment of unmanned aerial systems (UAS) and drones, focusing on the critical evolution of machine autonomy. A structured framework is presented to evaluate the transition of human oversight across the autonomy spectrum: from Human-In-The-Loop (HITL), through Human-On-The-Loop (HOTL), to the highly debated Human-Out-Of-The-Loop (HOOTL) architectures. The operational efficiency and ethical implications of delegating lethal and non-lethal decision-making to autonomous entities are critically assessed.

Keywords: autonomous systems, resilient communications, artificial intelligence, human-machine teaming

WORKING GROUP 4:
LEADERSHIP, COMMAND-AND-CONTROL, AND BASIC COMPETENCIES

Chair

PETRUS HENDRIKUS JOHANNES OLSTHOORN
Netherlands Defence Academy

Co-Chair

TOMMASO FORMATO
Baltic Defence College

RAWAAH ALMAHASNEH*

FROM VIRTUAL SIMULATION TO OPERATIONAL REALITY: INTEGRATING VR TECHNOLOGIES INTO CRISIS MANAGEMENT AND JOINT SECURITY TRAINING

*Jordanian Civil Defense

When a major crisis hits, seconds count, and the pressure on first responders and security forces is immense. Today's fast-moving threats demand flawless inter-agency coordination, yet traditional field training and live-fire drills face harsh limits. They are expensive, carry safety risks, and simply cannot safely replicate low-frequency, high-consequence catastrophes – such as a major aircraft accident or critical infrastructure failure. This paper explores how Virtual Reality (VR) and advanced simulation can transform the way we train the human beings tasked with managing these extreme events.

Rather than examining abstract theories, this study reviews international best practices to assess how immersive simulation impacts human performance under pressure. It examines how VR environments help personnel manage high cognitive loads, maintain spatial awareness, and communicate clearly when teamwork is most tested. By bridging the gap between tactical frontline decisions and strategic oversight, these technologies offer a safe space to fail, learn, and adapt.

The insights show that while virtual simulation can never completely replace physical experience, it drastically improves "first-pass" success, sharpens decision-making, and standardizes joint responses. Ultimately, this paper proposes a practical, cost-effective framework for security institutions to adopt simulation technologies – turning real-world operational insights into genuine defense innovation where it matters most: saving lives and building national resilience.

Keywords: crisis management, virtual reality (VR), inter-agency coordination, tactical training, human performance, defense innovation, first-pass success, national resilience

BARIŞ ATEŞ*
SELÇUK CANTÜRK[2]

HEROIC COMMAND AND THE COSTS OF FRONTLINE LEADERSHIP: COMMAND CULTURE IN THE TURKISH MILITARY

*-[2]Turikish National Defence University

This presentation explores how the command culture within the Turkish Armed Forces influences the relationship between leadership, risk, and military effectiveness. It highlights a prominent normative ideal within Turkish military culture: the expectation that officers should lead from the front, demonstrate personal courage, and exhibit moral authority by being physically close to danger. While this heroic model may enhance cohesion, trust, and fighting spirit, it can also lead to undesirable operational costs. These costs include commanders being exposed to preventable casualties and a failure to distinguish between inspirational leadership and unnecessary tactical exposure.

The study is based on an ongoing qualitative study that draws from Turkish military memoirs, war narratives, professional writings, and interviews. It specifically focuses on incidents where officers' behavior is praised, criticized, or mythologized. The article conceptualizes "heroism" as an institutional norm that is reinforced through training, commemorative ceremonies, promotion criteria, and exemplary command narratives. The analysis examines when being present on the front line serves as an essential leadership function, when it devolves into performative heroism, and how these boundaries vary across conventional, counter-terrorism, and technology-enabled operational environments. By linking operational experience to organizational adaptation, the article contributes to discussions on leadership, command-and-control, and military training.

Keywords: Turkish military, command culture, officer casualties, heroic command

JULIA BANAŚ*

KNOWLEDGE TRANSFER IN CONTEMPORARY SECURITY GOVERNANCE: A DISCOURSE-DRIVEN ANALYSIS OF NATO, EU, AND UN RECOMMENDATIONS

*The Polish Forum of Young Diplomats

In the context of rapidly evolving security environments and growing multi-domain complexity, NATO, the European Union and the United Nations increasingly emphasise the need to transform how security-related knowledge is generated and shared. This paper analyses how their strategic discourses and policy recommendations shape emerging models of knowledge transfer crucial for resilience, interoperability, and adaptive capacity in defence institutions.

Using Critical Discourse Analysis and a Systematic Literature Review of documents published between 2016 and 2026, the study identifies three core discursive orientations. NATO highlights resilience, interoperability and knowledge integration across multi-domain operations, stressing protection of critical infrastructure, countering information manipulation and the use of disruptive technologies in training and decision-making. The EU focuses on complementarity with NATO, strengthening defence-industrial capacities, countering hybrid threats, and developing shared analytical and training mechanisms, as reflected in the Strategic Compass and EU-NATO progress reports. The UN promotes inclusive, multilateral knowledge-exchange models grounded in international law, capacity-building, and civil-military cooperation.

Across all three organisations, a common trend emerges: a shift from hierarchical, static educational models toward dynamic, networked and iterative knowledge ecosystems that integrate operational data, predictive analytics, multi-domain simulations, and co-creation practices involving practitioners, analysts, and decision-makers. NATO and EU recommendations particularly emphasise interoperable learning structures enabling rapid updates and cross-institutional dissemination.

The paper proposes the analytical framework “tri-organisational knowledge pathways”, illustrating how NATO, EU, and UN discourses collectively shape the future of military education, decision-making and capability development. Effective knowledge transfer in multi-domain environments requires not only technological innovation but also discursive coherence, shared standards and common mechanisms for interpreting emerging threats.

Keywords: knowledge transfer, multi-domain operations, interoperability, critical discourse analysis

ERIC BÉGIN*

REIMAGINING CANADIAN NCM PROFESSIONAL MILITARY EDUCATION FOR 2035

*Canadian Defence Academy

Contemporary conflicts are reshaping defence transformation, from multi-domain operations and hybrid tactics to technological acceleration, ethical complexity, and the translation of battlefield lessons into education. This paper argues that Canadian Non-Commissioned Member (NCM) Professional Military Education (PME) must be reimagined for 2035 as a mechanism through which operational insight becomes defence innovation. The argument is built around two pressures. First, time compression creates an experiential gap: the CAF can no longer assume it has 10 to 15 years to produce experienced sergeants, warrant officers, and senior NCMs through linear occupational socialization. Second, scaling through expansion and mobilization brings more personnel, dispersed formations, accelerated training demands, and greater organizational complexity, making the cohesion, coordination, and connective functions of the CPO1/CWO Corps [OR-9] more difficult and more strategic. The traditional "push" model of NCM development remains necessary but insufficient. Organized around courses, qualifications, HR competency frameworks, succession management, performance measurement, assessment, and rationalized progression, it provides standardization, accountability, and coherence. Yet it risks reducing professional development to what the system can define, deliver, measure, and certify. The paper proposes a modular, outcome-driven PME ecosystem. This "pull" model begins with what the 2035 force requires from NCMs and CPO1/CWOs: judgment, advisory capacity, cohesion-building, coordination, institutional translation, ethical reasoning, and the ability to transform operational lessons into practice. NCM PME is thus part of the human architecture that enables armed forces to learn, adapt, scale, and professionalize at speed.

Keywords: non-commissioned members, PME, Canadian Armed Forces

ANDRÉ KORSMO BERNTSEN*

RATIONALITY MOTIFS IN DECISION-MAKING THEORY AND PROFESSIONAL JUDGEMENT IN THE MILITARY

*Military Academy at ETH Zurich

Cognitive superiority is often treated as though it entails more explicit analysis, better procedures, more information, and tighter control. That assumption misclassifies rapid, experience-based recognition under uncertainty as something less than rational. Dual-process theory loads the evaluative weight of rationality onto slow, analytical processing and treats fast, experience-based processing as its absence. Rationality motifs include practical wisdom (Aristotle n.d.), formal rationality (Mongin 2000), bounded rationality (Simon 1955), heuristics-and-biases (Tversky & Kahneman 1974), ecological rationality (Todd & Gigerenzer 2007), tacit knowing (Polanyi 1983; Kuhn, 1962/1970), and situated expertise (Dreyfus 2004). These motifs coexist without a settled hierarchy. A decision deficient by an optimization standard may satisfy bounded, ecological, or tacit-knowledge criteria under time pressure, incomplete information, and task structure. Their coexistence exposes the dual-process binary as too coarse (Melnikoff & Bargh 2018). Recognition-primed decision-making (Klein et al. 2010) corroborates this point. Experienced actors recognize a situation from cues, generate a course of action, and test it through mental simulation. When classified as System 1, it appears pre-rational by the standards of deliberate analysis. RPD satisfices under cognitive constraint, exploits environmental regularities, and draws on experiential knowledge that resists explicit rule reduction. Professional military judgement is not less rational because it is compacted. Its rationality depends on the fit among cognitive processes, actors' experiences, task ecology, and operational tempo. Cognitive superiority is not a property of the deliberate mode. In operational settings, the most rational actor is the least dependent on deliberation.

Keywords: recognition-primed decision making, rationality motifs, professional military judgement, dual-process theory, military education

OLGA CHIRIAC*

HUMAN ENCODING SCALE VERSUS ARTIFICIAL NEURAL NETWORKS: IMPLICATIONS FOR THE NATO COMMAND-AND-CONTROL ENTERPRISE

*Irregular Warfare Initiative

The rapid development of artificial intelligence (AI) is leading to major changes in the field of security and defense policy. AI serves as the cognitive anchor of robotics, thereby providing machines with cognitive capacities that have thus far been exclusively human, such as perception, decision-making, memory, and learning from experience. Naturally, alongside said technological progress came mainstream discussions surrounding the use of unmanned systems by the military. Nonetheless, most discussions are built around the technical dimension, acquisition flows and logistics, policy implications, or ethical boundaries. The present article focuses on the effects of AI (both LLMs and agentic) on command-and-control and military leadership. Present research makes a scientific attempt to reconcile artificial and human intelligence in the command-and-control dimension of operational art. The central source of data is operational insight acquired during a NATO exercise focused on seabed surveillance missions as well as battleground insight. The acquired data was applied to the human cognitive framework and cross-referenced with NATO command-and-control protocols. The aim of the article is to address questions of human-AI teaming and to outline possible implications for how professional military education (PME), recruitment, operational training, mission architecture, and strategic foresight could adapt to such novel opportunities. The article also outlines several human vulnerabilities in said space. A major contribution of our research is the comparative analysis of the human encoding scale to artificial neural networks encoding, storing, and information processing. The analysis factors in the impact of contextual meaning, multi-sensory depth as well as biological scaling. The findings of the present research are relevant to the wider NATO command-and-control enterprise, as well as to the armed forces of individual member states.

Keywords: agentic, cognition, decision making, mission command, NATO

WILLIAM COMBES*

COMMAND FIRST: AI IN THE HUMAN LOOP FOR COMPLEX OPERATIONAL ENVIRONMENTS

*Baltic Defence College

Military and security organizations increasingly field AI decision aids built for complicated problems, such as pattern matching, data correlation, and option generation, while operating in complex environments, where cause and effect become clear only in retrospect. This mismatch creates risk: analytical outputs get treated as answers when they are, at best, inputs to human judgment. The risk is hard to detect because AI conceals it behind fluency and confidence, whether the underlying problem is simple or complex.

Models, frameworks, and AI systems are instruments of the complicated domain. Each codifies known relationships and extrapolates the already-known, which is why none can navigate genuine novelty. That work belongs to human judgment, exercised not as a single decisive call but as probing, sensing, and adapting as a situation reveals itself.

In a decision system, AI sits inside the human loop. Command decision systems are not weapons systems and treating them alike distorts how AI is used for command. A decision aid does not act; it informs, working within the commander's judgment, which drives the cycle. This tracks a doctrinal boundary. Command, meaning authority, responsibility, and decision, is complex work and stays human. Control, meaning sensing, processing, and coordination, is complicated work and is open to AI. This boundary can blur where staff interface with the tools, and the effect carries upward, so the human-owned loop has to hold at every level.

Three patterns operationalize AI in the human loop: Adaptive Command (humans set intent; AI extends sensing), Strategic Sense-Making (AI surfaces patterns; humans determine meaning and frame the mission), and Ethical Responsibility (AI generates options; humans own consequences). The patterns are fractal, recurring from staff cell to commander. Command first, mission follows, conducted ethically.

Keywords: human-AI collaboration, command-and-control, complexity, military decision-making

DAVID GETSADZE*

AGENTIC AI FOR TOTAL DEFENCE: TRANSLATING OPERATIONAL LESSONS FROM UKRAINE INTO RESILIENT COMMAND-AND-CONTROL FOR SMALL DEMOCRACIES

*Business and Technology University; Ministry of Defence of Georgia

The war in Ukraine has fundamentally reshaped the landscape of modern warfare, demonstrating the critical importance of decision speed, information dominance, and societal resilience under hybrid and conventional pressure. For small democracies on Europe's eastern flank – including the Baltic states and Georgia – these operational lessons carry existential implications. Yet, while the literature on agentic AI in defence is rapidly expanding, it remains almost exclusively focused on great power competition and large military establishments. The GCSP (2026), CSIS (2025), and DoW strategic assessments address agentic AI's transformative potential for decision dominance and C2 compression – but the specific challenge of small democracies remains a critical gap in the literature.

This paper addresses that gap directly. It proposes a conceptual framework for integrating agentic AI into total defence architectures of small democracies: states characterised by limited defence resources, high hybrid threat exposure, deep societal mobilisation requirements, and dependence on allied interoperability. Drawing on operational insights from Ukraine – drone warfare, distributed C2 resilience, civilian-military coordination – and the Baltic total defence model, the paper identifies three critical capability gaps that agentic AI can address: fragmented situational awareness across civil-military boundaries, decision latency under hybrid threat saturation, and the absence of scalable early-warning mechanisms adapted to small state defence establishments.

The paper then develops a governance framework ensuring human oversight, algorithmic transparency, and clear accountability chains – allowing small democracies to deploy agentic AI capabilities without compromising democratic control or NATO interoperability standards. Georgia is presented as an illustrative case: a small democracy facing persistent hybrid threats, with constrained resources, seeking Euro-Atlantic alignment while developing indigenous resilience.

This paper argues that agentic AI, properly governed, is not merely a capability multiplier but a strategic enabler for small democracies – transforming battlefield and hybrid threat insights into future-ready, resilient total defence innovation.

Keywords: modern warfare, total defence, agentic artificial intelligence

SWATI KARAL*
ASHU PASRICHA[2], RUPANE GOYAT[3]

FROM INSIGHTS TO INNOVATION: RETHINKING COMMAND, LEADERSHIP IN AI ASSISTED WARFARE

*Central University Haryana, [2–3]Panjab University

The modern era of hybrid warfare is based on the integration of conventional use of force with cyber operations, proxy engagement, and disinformation. Artificial Intelligence-assisted technologies stimulate the speed and opacity that reduces the chances of threat deception and interception. The increased deployment of advanced technologies in modern warfare places a significant strain on military command, control and leadership. The existing studies emphasize command, control while considering hybrid threats, and AI assistance as a separate domain to be studied. However, limited research has been conducted to inquire how decision-making led by conventional insights is insufficient to address modern technology. Drawing on the illustrative cases of hybrid warfare involving AI in defence operations, the study highlights the research gap that present structures of command-and-control, policy frameworks are shaped by rigid hierarchical control, subjectivity in human judgements and values, making them highly unsuitable for an AI-enabled environment. The paper argues that a paradigm shift is required in defence policy by connecting operational insights to the developing capabilities of military leadership and to the adaptability in decision-making by changing the institutional framework of analysis. The study contributes to research on bringing innovation in defence, action-based insights for military educators, and policy enthusiasts, translating into future-ready action frameworks.

Keywords: command, control, decision making, military leadership, defence policy, hybrid warfare, AI-assisted

KHYATI SINGH*

BRIDGING THE GAP – OPERATIONAL FEEDBACK AS THE ENGINE OF DEFENCE INNOVATION

*MP-IDSA

The rapid evolution of modern conflict requires a paradigm shift in how military institutions process information. No longer can “lessons learned” be relegated to post-conflict analysis; instead, the integration of *operational insights* must become a real-time driver for *defence innovation*. This paper/presentation explores the mechanisms through which contemporary battlefield dynamics – characterized by multi-domain friction and high-attrition electronic warfare – are synthesized into systemic advancements in military science.

By examining the intersection of tactical experience and academic rigor, this session addresses how military sciences serve as the connective tissue between the front lines and the design bureau. We will analyze the specific pathways through which kinetic realities inform technological development, ethical legal adaptations, and the evolution of military education. Ultimately, the work argues that the agility of a nation’s defence posture is directly proportional to its ability to transform raw operational data into actionable, innovative doctrine.

Keywords: defence innovation, operational insights, multi-domain warfare, military science, tactical adaptation

CYRILL KISCHEL*

THE IMPORTANCE OF THE HUMAN LAYER IN AN INCREASINGLY AUTOMATED OODA LOOP

*Military Academy at ETH Zurich and Swiss Armed Forces

Among the latest innovations in the defence sector, autonomous systems, unmanned aerial vehicles, and electronic warfare capabilities directly on the tactical front line are becoming increasingly prominent. Whilst these technological advances accelerate data collection, they simultaneously shorten sense-making timeframes and shift the greatest vulnerability of the battlefield to the cognitive limits of the unit commander. This dynamic leads to a critical bottleneck, in which the machine speed regularly exceeds human processing capacities.

To address this challenge, this paper develops a conceptual model of the human element within AI-supported OODA loops, specifically tailored to the company level. Building on a literature review of OODA loops, cognitive workload, and socio-technical systems, the study introduces a mathematical framework to formalise how event density, resource diversity, and data latency exacerbate the cognitive load on a unit commander. This algebraic foundation serves as a theoretical prerequisite for subsequent computer-based simulations and empirical stress tests.

The contribution of this study is threefold. Firstly, it applies socio-technical framework concepts from the macro-level to the tactical micro-level, thereby defining the specific cognitive demands faced by unit commanders. Secondly, it provides an innovative mathematical model that isolates the command element to a single human node and demonstrates how machine-driven event velocity and resource diversity trigger a non-linear breakdown of situational awareness, which is attributable to intra-cognitive saturation and data-filtering latencies within the orientation phase of the OODA loop. Thirdly, it provides actionable insights for armed forces operating in a multinational integrated environment, demonstrating that the successful operationalisation of technological innovations depends entirely on the design of decision-making environments that consider the limited cognitive boundaries of human beings. Ultimately, the article concludes that tactical effectiveness in future high-intensity conflicts depends less on maximising data volume than on the mathematical optimisation of the balance between technological speed and human command limits.

Keywords: human layer, OODA loop, unit command, socio-technical systems, mathematical modeling

RENATO KLOSS*

FIT FOR PURPOSE: DOCTRINAL IMPLEMENTATION OF ROBOTIC AND AUTONOMOUS SYSTEMS FROM THE LESSONS OF UKRAINE AND GAZA

*Brazilian Army Command and General Staff College (ECEME)

Robotic and Autonomous Systems (RAS) are no longer marginal tools on the battlefield. Their growing use has made human-machine teaming a central issue for military doctrine, especially on command, targeting, force protection, and future operations. Wartime lessons in Ukraine and Gaza show how the demand for battlefield efficiency accelerated the rise of RAS, yet technology alone is not decisive. Lessons become capabilities only when doctrine turns them into standard practice. Ukraine and Gaza show how RAS are reshaping combat and why their enduring military value for future war depends on doctrinal adaptability. This paper seeks to translate those lessons into an analytical framework, so armies can institutionalise battlefield innovation and prepare for future conflicts.

Among several examples, Ukraine shows how drones can compress the kill chain through integrated networks, intelligence, and command, moving doctrine away from platform-centred thinking toward multi-domain integration. Gaza brings a different lesson in AI-assisted targeting doctrine. It must be regulated not only in terms of human oversight, but also in terms of its quality, with verification procedures, decision timelines, training against automation bias, and clear accountability.

Towards a credible doctrine that embraces RAS and its interoperability, armies need a process that keeps pace with technological change. This means doctrine should move through an iterative spiral, not a straight path from acquisition to doctrine. Autonomous technologies evolve too fast for that. NATO's CD&E process offers a starting point. Concepts are developed, tested, evaluated, adjusted, and then turned into doctrine. A solid doctrine defines not just the acceptable levels of autonomy, but the standard of human judgment required, review and override procedures, and responsibility across the kill chain. An effective RAS integration needs dedicated structures, shared training standards, guidance for offensive and defensive uses, and compliance with international humanitarian law. A fit-for-purpose doctrine must absorb battlefield lessons, guide commanders, and preserve human accountability.

Keywords: robotic and autonomous systems, military doctrine, Ukraine, Gaza, technology

MICHELE MASTROENI*

EMPOWERMENT FOR ADDRESSING COMPLEXITY IN THE ARMED FORCES: REFRAMING THE LEADERSHIP ANALOGY

*OCAD University

The presentation will outline a new metaphor for leadership, reframing the traditional “top-down” structure and command pyramid to one that allows for empowerment “up to” enlisted members and junior officers. In the application of design thinking to defence and security (i.e. military design), success in developing novel and innovative solutions to complex problems depends on the ability to explore and reframe problems and move beyond command’s initial identification of the problem, searching for the systemic roots of a problem rather than being stuck on a visible symptom. While to some the application of design thinking and the ability to question and reframe rests at the highest ranks, the Canadian Armed Forces have begun providing training in design thinking at the mid-ranking officer level and to senior non-commissioned officers (NCOs). We argue that there is room for greater exposure to design thinking across ranks, while respecting the need for technical training, experience, and military hierarchy.

Through insights gathered from approximately 40 interviews with officers and NCOs, we will indicate the challenges to design thinking and the perception of agency that members of the armed forces struggle with (regardless of rank) when dealing with complex problems, how regardless of these challenges design thinking has fit and been used successfully to come up with solutions to complex problems, but more importantly how reimagining a metaphor for leadership can improve its application and the application of devolved/decentralized command. From a top-down pyramid to a strong tree where leaders provide the roots and flow of support upward to all members, reframing leadership is a first step toward greater effectiveness and buy-in by military members in an environment troubled by both increased security threats and recruitment and retention challenges.

Keywords: leadership, design thinking, metaphors

KEVIN MATHERS*

STRATEGIC MISSION COMMAND IN NATO: INFLUENCE, SENSING, AND THE HUMAN DIMENSION

*Canadian Armed Forces

This paper examines a central challenge in contemporary coalition warfare: how NATO achieves unity of effort when unity of command cannot be assumed. Drawing on my experience as the Allied Command Operations Command Senior Enlisted Leader (ACO CSEL), the work argues that the decisive factors in strategic mission command are human, relational, and influence-based rather than structural or doctrinal. NATO's environment, shaped by sovereignty, national caveats, uneven capabilities, and diverse military cultures, creates persistent seams where formal authority cannot fully reach. As noted in the paper, 'coalitions rarely break at the centre; they fracture at the handoffs', and it is within these handoffs that senior enlisted become strategically consequential. The paper highlights how the ACO CSEL role functions as a sensing mechanism, identifying early indicators of readiness, morale, and operational friction that rarely surface through formal reporting. One example describes how a critical equipment gap, invisible in staff processes, was surfaced through leader-line relationships and resolved discreetly, 'preserving national dignity while restoring genuine readiness'. The paper introduces a practical framework that illustrates the interaction between the command-line (formal authority) and the leader-line (professional influence), arguing that mission command at the strategic level emerges at the intersection of these two lines.

The paper concludes that NATO's strategic strength lies in people, particularly senior NCMs who sense friction before it becomes failure and translate political decisions into disciplined action across diverse national forces.

Keywords: senior enlisted leadership, mission command

NIKOLAOS MITROPOULOS*

OPTICS OF MODERN CONFLICTS: HOW INFORMATION DISORDER LEADS TO DEFEAT AND PRACTICAL SOLUTIONS FOR LEADERS

*Hellenic Army and Neapolis University

"You can win a battle and lose the war on the evening news" - Edward Luttwak

How does a democratic nation react when the images returning from the Vietnam War offend its sensibilities? How do you prevent negative publicity while fighting a war for survival when you are beholden to the support of your allies to provide material and ammunition to your front line in the Donbas? How do you maintain the grace of the international community when unruly troops represent you poorly by their actions in the Gaza Strip?

In a world where every combatant and civilian carries a camera, where media literacy is failing to keep up, in a world of Information Disorder, how do you maintain the necessary image?

This paper aims to use a qualitative approach to an old problem, greatly amplified by modern technology: How are commanders to lead at the tactical, operational, and strategic levels to uphold the optics necessary to maintain morale and support for their side in a conflict?

It mainly analyses Russian information warfare used against neighboring states and the Eastern Flank of NATO as well as attempts to offer solutions to the problem of modern technology being used as a tool of disinformation, misinformation, and malinformation for large-scale distortion of public perception and demoralization.

Keywords: optics, information disorder

JOHAN ÖSTERBERG*
ANDREAS EDEVALD[2]

THE JANUS FACE – A METAPHOR FOR INFORMATION INFLUENCE AND COGNITIVE BIASES

*-[2]Swedish Psychological Defence Agency

This presentation concerns the inherent duality of repetition in human cognition, drawing parallels to the Roman god Janus, who looks to both the past and the future. Repetition is foundational to learning and memory (‘Repetition is the mother of knowledge’), yet it also makes individuals and societies vulnerable to deception (‘If a lie is repeated often enough, it becomes true’). Furthermore, the study explores key cognitive biases – illusory truth effect, confirmation bias, motivated reasoning, and knowledge neglect – that explain why repeated false information can gain traction. Critically, the rise of Artificial Intelligence (AI) is presented as a ‘Janus-faced’ tool, capable of vastly amplifying both the positive and negative impacts of repetition. While AI can exacerbate the spread of disinformation through mass generation, targeted influence, and algorithmic reinforcement, it also holds significant promise as a tool for debunking, critical thinking education, and understanding cognitive vulnerabilities. The core message is that confronting these challenges requires a conscious effort to overcome cognitive biases, robust media literacy, and the ethical, interdisciplinary application of AI.

Keywords: repetition, cognitive biases, information influence, artificial intelligence

SOILI PAANANEN*

MILITARY LEADERS AND COMPLEXITY - STRATEGIC LEVEL VIEWPOINT

*Finnish National Defence University

The paper examines the complex situations faced by military leaders. The phenomena under investigation are related to the processes of work activities and collaboration. By focusing on complex situations, the paper will provide insights into what complexity means in the work of military leaders and how they strive to resolve issues and phenomena they perceive as complex in an adaptive, innovative, or holistic manner.

The research methodology employed is ethnography, aiming to understand the cultural phenomenon of complexity and its solutions in a crisis-simulating environment from the perspective of military leaders. The research context is an international staff exercise. The research methods include participant observation, note-taking, document analysis, and discussions with group facilitators and students.

The paper will produce comprehensive knowledge and recommendations for the development of leadership training.

Keywords: complexity, military leader, international staff exercise

PIER-AUDREY BONNIER *
DAVID BÉLANGER[2]

WOMEN IN LEADERSHIP ROLES IN THE CANADIAN ARMED FORCES

*-[2]Non-Commissioned Member Leadership College

Starting in 1885, Canadian women integrated the Canadian military as nurses. During World War 1, World War 2, and the Korean War, women's roles in the Canadian Armed Forces (CAF) expanded beyond nursing into clerical and administrative positions, even though their domain remained within the care paradigm. In 1989, all occupations in the CAF became accessible to women, including combat roles, yet they are still encountering obstacles regarding equity and equality today. Evolving from an environment that is structurally women-averse to a continual increase in the representation of women in the CAF raises questions about women's participation and contribution to the profession of arms. At the center of a profound cultural shift in recent years, the Department of National Defence (DND) aims to change its culture, which is reflected in particular by having higher quotas for women in the CAF. They are now becoming figureheads of inclusivity and equality, the representation of tokenism of these cultural changes. From there, a political and normative message has been attached to the feminine gender in the CAF, changing how they are perceived as a part of the Forces. In this context, we are presenting Canadian women in leadership roles within the CAF, more specifically, senior enlisted leaders (Non-Commissioned Members in Canada). This article will bring together their vision on how gender, authority, and professional identity intersect within senior enlisted leadership roles in the CAF. This will also be the opportunity to explore how women offer different types of leadership than men in terms of cohesion, mentorship, and operational effectiveness, to name a few, in their experience of relational expertise. This will present a meaningful occasion to study the contrast between Canadian practices and practices found elsewhere, by using external examples of how women's leadership is used in military operational contexts.

Keywords: armed forces & society, women in leadership, operational effectiveness, culture change, identity

CEMIL SAĞLAM*

FROM THE FIELD TO REFORM: THE PROFESSIONALIZATION EXPERIENCE OF THE TURKISH ARMED FORCES THROUGH SPECIALIST SERGEANTS

*Turkish National Defense University

The shifting security environment of the twenty-first century has driven states to redesign their military structures, from recruitment policies to the definition of duties. Since the early 1990s, the Turkish Armed Forces (TAF) has likewise moved toward a hybrid model that combines conscription with professional personnel, shaped by intensifying counter-terrorism operations and cross-border missions. One of the most concrete outcomes of this transformation is the specialist sergeant (*uzman erbaş*), today one of the largest combat groups within the TAF. This paper treats the experiences of these key actors on the operational front as a source of knowledge that illuminates defence transformation.

The data draw on the author's doctoral dissertation, conducted using a mixed-methods design: in-depth interviews with 32 former specialist sergeants were subjected to thematic analysis and integrated with survey data collected from 387 participants. The findings show that the rapid expansion of the system in response to urgent operational needs has generated a number of structural problems in the field. Factors such as ambiguity in the definition of duties and weak occupational security foster a sense of belonging that is "committed yet resentful", along with institutional alienation; these in turn drive attrition and make it difficult to retain hard-won operational experience within the institution.

In conclusion, the experiences of specialist sergeants are not merely an individual matter but a concrete site of learning for transforming personnel policy.

Keywords: Turkish Armed Forces, specialist sergeant, professionalization

ROCCO PASCO SANTURRI III*

FROM SEOUL TO THE SUWALKI GAP: A UNIFIED COMMAND BLUEPRINT FOR THE BALTICS

*United Nations Command

Context and problem: With the transition from tripwire deterrence to deterrence by denial, NATO faces significant command-and-control (C2) issues stemming from inherent multinational friction. Potential Russian aggression on NATO's eastern flank demands rapid, seamlessly integrated response capabilities unburdened by multi-state coordination and bureaucracy. An advanced integrated deterrence model is needed.

Methodology and cultural analysis: This submission provides a comparative analysis between the ROK-US Combined Forces Command (CFC) and nascent multinational Baltic defence initiatives. It examines the CFC as a potential structural model for a unified Baltic Command. Beyond military utility, this paper utilises a human terrain analytical perspective that puts forth an unexpected thesis: the Baltic States are better suited to employ the CFC model than the ROK, given the Baltic's existing NATO interoperability and acceptance of Western military collaboration, and South Korea's societal structure and cultural history. Furthermore, the Baltics are inherently well-positioned to move beyond the CFC model and capitalize on the attributes of ROKUS Mission Command structure while avoiding the detrimental integrational aspects exposed in the Korea theatre.

Innovation and conclusion: this paper proposes a significant defence innovation based upon the operational insights from the ROK-US blueprint: a permanent, enduring, and agile Combined Baltics Command. Additionally, the current ROK-US OPCON transition demonstrates how tightly integrated, multinational commands can be designed to support host-nation sovereignty. This comparative analysis provides a doctrinal foundation and actionable trajectory for a resilient, integrated, and unified defence architecture better suited to deter the Russian threat on NATO's eastern flank.

Keywords: C2, command, control, integration, friction, blueprint

EVA SULA*

THE INTEGRATION GAP: WHY OPERATIONAL LESSONS RARELY BECOME OPERATIONAL CAPABILITY

*Independent Defence & Security Advisor

Defence organisations invest significant effort in exercises, operational analysis, experimentation, and lessons learned processes. At the same time, innovation programmes, procurement initiatives, and capability development efforts continue to accelerate across NATO and partner nations. Despite these activities, a persistent gap often remains between lessons identified and capabilities fielded.

This paper examines the integration gap: the disconnect between operational insights and their translation into usable, sustainable military capability. While technology is frequently presented as the primary solution to emerging challenges, many failures occur elsewhere. Capabilities do not succeed solely because systems are procured or prototypes are demonstrated. They succeed when technology, doctrine, training, processes, governance, and organisational structures evolve together.

Drawing on observations from defence, government, and innovation ecosystems, this paper explores recurring barriers that prevent operational lessons from becoming operational outcomes. These include fragmented ownership, competing priorities, organisational silos, insufficient user involvement, and the tendency to treat procurement as the end of capability development rather than its beginning.

The paper proposes an integration-focused framework for capability development that connects operational users, innovators, industry, and decision-makers throughout the lifecycle of a capability. Particular attention is given to the role of leadership, command structures, and organisational learning in enabling adaptation.

The findings suggest that the challenge facing modern defence organisations is not a shortage of innovation or lessons identified. The challenge is the ability to integrate those lessons into doctrine, training, processes, and operational systems at sufficient speed and scale. Understanding and addressing this integration gap is essential for maintaining readiness and translating insight into military advantage.

Keywords: capability development; lessons learned; military innovation; C2, organisational learning; defence transformation; operational readiness; defence leadership

JANNE TÄHTINEN*

KEY TENETS OF NATO'S ALLIED JOINT DOCTRINE AND MDO

*Finnish Defence Research Agency

This presentation is based on a work-in-progress article that examines the four key tenets contained in NATO's Allied Joint Doctrine in relation to multi-domain operations and considers their implications for the art of war. The doctrinal tenets are comprehensive approach, manoeuvrist approach, behaviour-centric approach, and mission command.

The article assumes that NATO's implementation of the MDO concept is grounded in the doctrinal tenets elevated to a central role in the doctrine – or, at the very least, that these tenets provide a useful framework for understanding the Alliance's thinking on multi-domain operations. The article, in particular, reflects the Finnish art of war, but the findings can be applied more generally as well.

The study found that the foundation of MDO in NATO stems from the tenet of the comprehensive approach. This is understandable given the nature of the Alliance. The comprehensive approach is emphasised at the strategic and operational levels, integrating all instruments of national power as well as military and non-military actors. At the strategic level, the objectives and the enabling conditions for MDO are established.

Multi-domain thinking conceptualises the battlespace at the operational-tactical level into physical, virtual, and cognitive dimensions, which reflects both the manoeuvrist approach and the behaviour-centric approach. The relative advantage required to defeat the adversary is achieved by concentrating effects across all dimensions (convergence) against identified adversary vulnerabilities, as well as against cohesion and will.

Multi-domain operations place particular emphasis on achieving shared situational understanding and on enabling initiative-driven decision-making for the execution of military operations. Mission command – centralised planning combined with decentralised execution – has been viewed as challenging in MDO. However, understanding the commander's intent at higher echelons enables innovative and proactive action at lower levels also in multi-domain operations. This nevertheless requires sufficient cross-domain coordination and command capabilities at lower-level command posts.

Keywords: key tenets, MDO, art of war.

KIRSTEN WILD*
SARA RUSSO[2]

COGNITIVE WARFARE, OODA LOOP, STRATEGY, AND DECISION-MAKING

*University of Poitiers, [2]University of Turin

Targeting Orientation and Decision-making: Cognitive Tunnels and the Degradation of Strategic Agency through Cognitive Warfare Contemporary research on cognitive warfare and Foreign Information Manipulation and Interference (FIMI) has increasingly highlighted how sustained influence environments may affect institutional trust, collective sense-making, and decision-making processes. While existing literature predominantly focuses on content manipulation and narrative dissemination, less attention has been devoted to how such environments may progressively constrain institutional orientation itself, meaning the interpretive processes through which actors construct situational awareness and generate actionable responses.

This analysis presents a theoretical contribution through an integrative literature review, synthesising perspectives from cognitive science, strategic studies, and research on cognitive warfare. It refers to the concept of *cognitive tunnels* (CR451) as a heuristic construct for analysing how sustained informational pressure may progressively narrow interpretive space and reduce strategic flexibility within institutional environments.

Drawing on the "Orient" phase of Boyd's OODA loop and broader perspectives on sense-making and strategic cognition, the paper examines how contemporary influence operations and high-pressure information environments may disproportionately affect processes of perception, interpretation, and situational framing rather than persuasion alone, thereby degrading the conditions under which strategic agency is exercised. Proposed mechanisms include emotional intensification, narrative convergence, adversarial identity framing, informational saturation, and sustained framing pressure.

Rather than directly imposing specific beliefs, such dynamics may contribute to narrowing the range of perceived alternatives and reinforcing reactive modes of decision-making.

The analysis further argues that similar dynamics may increasingly emerge within organisational and economic decision environments, where uncertainty shaping, reputational signalling, and perception management influence institutional behaviour and market responses. In contributing to debates on cognitive warfare, hybrid threats, and democratic resilience, the paper proposes orientation degradation as a theoretically generalisable phenomenon warranting systematic analytical attention across multiple domains.

Keywords: cognitive warfare, OODA loop, strategy, decision-making

WORKING GROUP 5:
MILITARY LAW AND ETHICS

Chair

OLAVI JÄNES
Baltic Defence College

Co-Chair

LENU ORG
Estonian Military Academy

GABRIEL MATTHEW BERGMAN*

SEMIOTIC SCAFFOLDING AND CHANGING VALUES: MILITARY PRAXIS IN THE AGE OF AUTOMATION.

*University of Tartu

This presentation aims to extend a 2019 study at a Brazilian military academy concerning cultural psychologist and semiotician Jaan Valsiner's model of affective semiosis in understanding the social values that define military praxis. In the study it was suggested that the "[military] Academy powerfully cultural[ly] canalizes individual experiences, through the insertion of redundant social suggestions regarding military values in various socialization practices" (Wortmeyer & Branco 2019: 600). In doing so, the authors argue that the primary pedagogical strategy employed by the instructors at the academy is one that emphasizes the construction of affective-semiotic fields related to the specific values of the nation's military community (Wortmeyer & Branco 2019: 595). These values have been referred to in other literature as "internal goods" (de Vries 2020). Internal goods, as they are being referred to in this context, can be defined as the guiding social values that practitioners of a certain type of praxis aspire towards and are not exclusive to military operations. In military praxis, these internal goods can be understood as "a sense of excitement, pride, and satisfaction" (de Vries 2020: 175). It has also been suggested, however, that the increased usage and reliance on automated systems has the potential to alienate service members from the internal goods or destabilize the pre-existing affective-semiotic fields that have been established and ingrained through their military training (Hasselberger 2024: 295). Additionally, this presentation will consult biosemiotician Claus Emmeche's notion of semiotic scaffolding of the social self (Emmeche 2015) in order to better understand the affective-semiotic model of military praxis. Ultimately, the aim of this presentation will be to showcase the significance of semiotic research methods and theory in investigating the question of the changing social dynamics of military praxis, in an era where an increased reliance on their usage can lead to a transformation in the socio-cultural values associated with being a service member.

Keywords: semiotics, law, military ethics, social values

SUMANTA BHATTACHARYA*
BHAVNEET KAUR SACHDEV[2]

ARTIFICIAL INTELLIGENCE-DRIVEN DEFENCE INNOVATION: TRANSFORMING OPERATIONAL DECISION-MAKING AND MULTI-DOMAIN MILITARY STRATEGY

*CENJOWS, [2]Suresh Gyan Vihar University

In the age of modern warfare, Artificial Intelligence (AI) is significantly transforming the nature of war due to its impact on operational efficiency, accelerated decision-making process, and military capabilities in all relevant domains, including land, air, maritime, space, and cyberspace. With the growing number of multidomain security challenges faced by the armed forces in terms of hybrid threats, cyberwarfare, autonomous warfare, and information operations, AI technologies have been recognized as important tools for defense innovation. This paper analyzes how AI transforms operational decision-making and its impact on situational awareness, mission planning, intelligence fusion, logistics, and other aspects of modern warfare. It further discusses strategic advantages and operational difficulties of implementing AI in order to transform military organizations. The paper focuses on the importance of reliable algorithms and cybersecurity issues, interoperability and compatibility of different technologies, ethical and legal concerns related to the implementation of AI solutions, as well as the use of AI as a force multiplier. Based on the contemporary literature review, the research proposes a framework for successful incorporation of AI in the decision-making process of the military organization. The current study adopts a qualitative and interdisciplinary approach and is based on the review of contemporary literature in defense and warfare, strategic policy documents of the military organizations, and recent military case studies.

Keywords: AI, warfare, defence, military organization, cyberwarfare, maritime

JAN ASMUS BISCHOFF*

LOST IN TRANSLATION? MILITARY CONCEPTS, DOCTRINE, AND THE CASE FOR COMPARATIVE MILITARY STUDIES

*NATO Joint Warfare Centre

International military cooperation requires understanding the other involved actors and their ways of doing things. Integration – be it on a bilateral or a multilateral basis, like in NATO – requires more: it requires a uniform terminology and doctrine. Doctrine does not come into life spontaneously. Generally, it is heavily influenced by the nations that participated in the drafting. But considering that English is NATO's working language, very often national concepts need to be translated into professional English military terms – terms which already have a specific meaning in respective English-speaking countries' militaries. The pre-understanding can be unconsciously imported when using such terms. Mission command, for instance, is one of NATO's key principles. Its roots can be traced back to the idea of *Auftragstaktik*, developed by the Prussian/German army in the late 19th century as a response to the commanders' inability to exercise close control over their forces. Mission command was adopted by the United States in the 1980s and then became part of NATO doctrine. Although there is a definition of mission command in NATO doctrine, soldiers from the United States and Germany apply their own national understanding of mission command (or *Auftragstaktik*).

Such problems are not unknown in the international arena. International legal harmonization, which began in the late 19th century, led to the creation of a new legal discipline: comparative legal studies. Comparative legal studies seek to understand the different legal systems (and families of legal systems). In doing so, they do not just compare the terminology (and its translation). They include legal history and social sciences to frame the factual problems addressed by certain legal rules. Without this academic work the far-reaching harmonization of law in the EU would have been impossible.

Hence, I argue that a separate academic discipline of comparative military studies with its own methodology needs to be developed.

Keywords: mission command, comparative military studies, NATO, doctrine

CAIO GRACO CAMPELO*

TEMPORAL COMPRESSION OF DETERRENCE: RETHINKING STRATEGIC STABILITY IN THE AGE OF ARTIFICIAL INTELLIGENCE

*Brazilian Naval War College

The integration of artificial intelligence into Nuclear Command, Control, and Communication (NC3) systems has generated renewed debate about the future of strategic stability. Existing scholarship often treats AI as either inherently destabilizing or potentially stabilizing, depending on its operational effects. This article advances a different argument: the strategic significance of AI lies not primarily in its impact on material force balances, but in how it reshapes the temporal architecture of deterrence. Drawing on classical deterrence theory and contemporary analyses of command-system vulnerability, the study introduces the concept of Temporal Compression of Deterrence (TCD), defined as a structural reduction in strategic decision-time produced by accelerated detection, data fusion, and decision-support systems. Through conceptual analysis and theoretical application to evolving NC3 architectures, the article demonstrates that accelerated informational velocity can intensify perceptions of vulnerability and crisis urgency even when second-strike capabilities remain materially intact. Stability, therefore, becomes conditional upon the preservation of deliberative space within increasingly accelerated systems. By foregrounding tempo as an analytical variable, the article refines classical deterrence theory and contributes to contemporary debates on AI, escalation risk, and nuclear governance.

Keywords: strategic stability, Nuclear Command-and-Control (NC3), artificial intelligence

SERAFIM CARVALHO*
MARIA COSTEIRA[2]

CRYPTOGRAPHIC VULNERABILITY AS HYBRID THREAT VECTOR: HOW POSTQUANTUM STANDARDISATION CHOICES SHAPE NATO'S EXPOSURE IN THE TRANSITION WINDOW

*-[2]Complear

Hybrid threats exploit gaps between institutional awareness and action. NATO's position, caught between legacy cryptographic infrastructure and incomplete post-quantum deployment, constitutes such a gap. The European Commission's proposed NIS2 amendments assess that harvest-now-decrypt-later operations are likely occurring now. Encrypted data is being collected for decryption when quantum capability matures. What remains missing is a governance framework to address this while the window is still open.

Post-quantum standardisation choices will determine that framework's shape. When NIST completed its first PQC standards in 2024, alliance convergence seemed plausible. In February 2025, China's Institute of Commercial Cryptography Standards launched a competing programme framed around technological sovereignty. For NATO allies, three positions present themselves: NIST alignment preserves interoperability but concentrates governance in a single ally; European alternatives trade dependency for fragmentation; legacy systems extend exposure indefinitely. Current NATO policy lacks any mechanism for choosing deliberately.

When cryptography fails, consequences cascade across domains. Compromised encryption exposes physical operations. Vulnerable identity verification opens classified installations to digital penetration. When biometric records, psychological assessments, and health data of military personnel are harvested under collect-now-decrypt-later conditions, adversaries gain medical intelligence enabling targeting and coercion. The evidence base is developing, but the threat's logical structure is established.

Drawing on practitioner experience in NIS2, GDPR, and classified matter compliance, this paper identifies where EU and NATO instruments leave the transition window ungoverned, examines what divergent standardisation means for allied digital sovereignty, and proposes a unified NATO transition governance doctrine.

Keywords: post-quantum cryptography, hybrid threats, NATO, digital sovereignty, critical infrastructure, intelligence, NIS2, transition governance

GITA LEITLANDE*

DEFENDING IN AN UNJUST WORLD

*National Defence Academy of Latvia

The ongoing war between Russia and Ukraine is a valuable source for lessons military scientists can derive from various angles, including the ethical dimension. This is especially relevant to European nations due to the war's geographic proximity, Russia's historical and current expansionism, and related rhetoric directed at Europe.

This study is the second step in the two-step study. The first step was to analyse whether Russia observes the 'Just War' principles during the Russo-Ukrainian full-scale war, which started in February 2022. It concluded that Russia is violating, by a considerable margin, the principles of just conduct in war, while having a strong narrative that supports Russia's conduct as at least somewhat permissible if not justifiable.

The second step, the current study, takes these conclusions from the first step as a departing point, and asks the question, so what: whether and how it impacts Europe's thinking and behaviour regarding Just War theory and preparing their military and societies? And, subsequently, what recommendations regarding policies and actions can Europe draw in light of Russia's widespread disregard for the Just War principles and its narrative that tries to portray that the opposite is true.

Taking into account the conclusions from the first step, this study is based on two assumptions. First, that Europe has a strong interest in the Just War principles remaining relevant and continuing to uphold them. And second, that Russia has not, is not, and is not going to respect Just War principles during any military conflict it is involved.

That's why there is room for military ethicists to help navigate between these two diametrically opposed stances regarding the observance of Just War principles: since European political decision-makers, societies, and military should be aware and prepared for that.

Keywords: Russia, just war theory, Europe, ethics

ASTA MASKALIŪNAITĖ*

MORAL SHIELD? LEGAL AND ETHICAL QUESTIONS OF TOTAL DEFENCE

*Baltic Defence College

As international relations become more unstable, more countries are reviving “old” ideas of defence. For the Baltic countries, Scandinavian approaches of comprehensive or total defence have become especially appealing, and they have begun implementing elements of these models in their defence preparations. While this preparation has advanced, one aspect of total defence remains marginal in discussion – the legal and ethical dimension. This dimension requires intense civilian participation in defence, which conflicts with the basic premise of international humanitarian law and just war ethics, both of which demand a distinction between combatants and noncombatants. Moreover, the IHL approach to civilian direct participation in hostilities appears to be interpreted broadly, potentially placing civilians who support national defence not only in harm’s way but also in legal jeopardy.

With this in mind, the legal and ethical aspects of total defence should be taken more seriously. If countries expect civilian participation, they should be clear about the legal consequences of such actions. Governments must be transparent with citizens, and total defence arrangements should be developed ethically. This implies mutual respect, dialogue, transparency, and solutions to the legal challenges such participation creates. Analyses of political duties and obligations may offer one path forward, while considerations of security ethics and state obligations offer another. States should also consider shaping international law to better protect civilians facing aggression, or alternatively, provide protection by more fully incorporating such civilians into the armed forces.

Keywords: total defence, DPH, political obligations, state obligations, civilian protection

IONELA-VALERIA POPESCU*
DRAGOȘ-GEORGE IONICĂ[2]

BETWEEN WAR AND PEACE: THE LEGAL ARCHITECTURE OF OFFENSIVE CYBER OPERATIONS UNDER INTERNATIONAL HUMANITARIAN LAW

*The Romanian National Cyber Security Directorate (DNSC), [2]Independent researcher

Offensive cyber operations (OCOs) have emerged as a defining instrument of contemporary statecraft, occupying a legally ambiguous space between peacetime espionage and armed attack. The proliferation of state-sponsored cyber intrusions, disruptive operations, and destructive malware – from the Stuxnet campaign against Iranian centrifuges to the sustained Russian cyber offensive against Ukrainian critical infrastructure – has exposed fundamental gaps in the international legal order governing the use of force. Existing frameworks, principally the United Nations Charter, customary international humanitarian law, and the non-binding Tallinn Manual on the International Law Applicable to Cyber Operations, offer partial but incomplete guidance, leaving military commanders, legal advisers, and policymakers without a coherent threshold doctrine.

This paper advances three principal arguments. First, the existing jus ad bellum threshold of 'armed attack' – predicated on kinetic analogies – fails to capture the graduated, deniable, and often dual-use character of offensive cyber operations; a new effects-based threshold doctrine is required. Second, the attribution challenge is not merely a technical or intelligence problem but a structural legal deficit that undermines the self-defence regime and enables a permissive environment for aggressor states. Third, the principles of distinction and proportionality, while theoretically applicable in cyberspace, require domain-specific operational interpretations to be practically enforceable, particularly given the interconnected nature of civilian and military digital infrastructure.

Drawing on the operational record of recent conflicts – including the Russo-Ukrainian war (2022-present), the NotPetya and Sandworm operations, and the Israeli-Iranian cyber campaign – this paper proposes a threshold framework integrating four criteria: effect severity, reversibility, civilian impact, and systemic disruption. The paper further argues for a multilateral attribution consortium as a functional substitute for unilateral state assertions and recommends doctrine-level proportionality guidance calibrated to cyber-specific civilian infrastructure dependencies. The analysis is addressed to both military legal practitioners and policy architects engaged in developing national cyber doctrines consistent with international law.

Keywords: offensive cyber operations, IHL, jus ad bellum, armed attack threshold, attribution, proportionality, Tallinn Manual, cyber warfare, critical infrastructure

AJSELA TOCI*

NARRATIVES OF SOVEREIGNTY AND TERRITORIAL INTEGRITY: A COMPARATIVE DISCOURSE ANALYSIS OF THE WESTERN BALKANS AND GEORGIA THROUGH INTERNATIONAL LAW AND POLITICAL ETHICS EPOKA

*EPOKA University and Wasatia Graduate School of Peace and Conflict Resolution (Europa-Universität Flensburg)

The tension between the legal principle of territorial integrity and the ethical–legal concept of self-determination remains a persistent source of friction in both the Western Balkans and the Caucasus. The Russian invasion of Ukraine has reshaped post-Cold War understandings of European security, altering how sovereign borders are contested, negotiated, and legitimised. This paper examines how different actors mobilise legal norms, political narratives, and ethical claims to justify or challenge territorial arrangements in Kosova and South Ossetia.

Using a comparative approach, the study analyses three categories of actors: local actors (Kosova and South Ossetia), regional actors (Belgrade and Tbilisi), and revisionist actors (the Russian Federation). The paper distinguishes between (1) legal principles, such as self-determination, territorial integrity, and humanitarian intervention; (2) political narratives, including ethnic protection, external self-determination, and sovereignty claims; and (3) ethical assessments of how these narratives are used to legitimise competing territorial claims.

In Kosova, the interaction between external self-determination and local security imperatives forms the core of its Euro-Atlantic integration narrative, while Belgrade continues to challenge Kosova's sovereign legitimacy. In South Ossetia, Moscow employs the language of ethnic protection and humanitarian intervention to justify border changes and territorial annexation, transforming legal concepts into instruments of hybrid warfare. The paper argues that contested borders in the Western Balkans and Georgia have become institutionalised zones of geopolitical confrontation. By comparing these cases, the study demonstrates how legal and ethical concepts are strategically deployed, and how the credibility of competing narratives shapes regional stability and the wider European security order.

Keywords: sovereignty, ethical, international order, Kosova, Post-Ukraine security

LINA VIDAUSKYTĖ*

A PHENOMENOLOGICAL ANALYSIS OF THE STRUCTURE OF DECISION MAKING IN AI SUPPORTED WARFARE

*General Jonas Žemaitis Military Academy of Lithuania

Contemporary armed conflicts increasingly rely on artificial-intelligence-based systems for planning and target selection. These developments are often described in the language of normative ethics, with references to responsibility, human involvement, or “meaningful human control”. However, such discussions rarely question whether the structure of experience in which these norms should operate still remains. A phenomenological perspective allows the issue to be addressed more deeply by examining how the experience of decision-making, action, and responsibility itself is being transformed. In AI-supported warfare, decision-making is marked by a radical compression of time. Operations are planned and executed within seconds or minutes, which removes the temporal space needed for deliberation and reflection. What was traditionally understood as a decision – an intentional human act – increasingly becomes the confirmation of an already prepared process. Action no longer appears as a decision grounded in experience, but as a procedural execution. This temporal crisis is clearly visible in recent conflicts. For example, at the beginning of the 2026 Iran conflict, nearly 900 strikes were carried out within the first twelve hours. Such an operational tempo marks a threshold beyond which meaningful human participation in ethical decision-making becomes structurally impossible. Here, speed functions not merely as a technical factor, but as an ontological limit. Human involvement does not disappear, but its form changes. Humans remain as functional points of authorization rather than intentional subjects of action. As a result, responsibility increasingly exists only at an institutional or discursive level. From a phenomenological perspective, the core problem of AI-supported warfare is not the absence of norms, but the transformation of the experiential conditions in which ethical judgment could meaningfully occur.

Keywords: AI-driven decision-making, operational speed, human agency, ethics of warfare, decision compression

AULI VIIDALEPP*
GABRIEL MATHEW BERGMAN[2]

TOWARD AN ETHICAL DESIGN FRAMEWORK FOR AUTOMATED FUNCTIONS IN MILITARY SOCIOTECHNICAL SYSTEMS

*-[2]University of Tartu

AI-enhanced systems (AIS) are designed to develop certain elements of *epistemically emergent behaviour***.** Consequently, the future behaviour of the system itself cannot be predicted with full certainty at the time of design. Due to the combined unpredictability of emergent behaviour and the human factor, it is likely that many issues will be revealed in testing and some only in a real-life operational context. This complicates the design process of any AIS, but especially the design of automated/autonomous functions in the military context.

In 2019, IEEE opened the discussion on the ethical design of AI systems, highlighting the need for *values-based design* and *stakeholder engagement.* In military technology, the development of automated weapons with greater autonomy necessitates that certain LOAC-compliance assessments be conducted before the operational phase. This requirement significantly widens the habitual stakeholder circle and changes the way in which automated or AI functions need to be designed. Various stakeholders must work together to achieve a product that fits regulations, stakeholder needs, and military and societal values. Facilitating this process is challenging on all levels.

The *Socio-Technical Feedback Loop* (SOTEF) framework (Heijnen et al. 2024) supports the design and development process of military AIS, considering intersections with various societal actors and institutions at four levels: governance, design, development, and operation. The framework also considers ethical, legal, and societal aspects (ELSA) of AI functions and the *continued democratic oversight* of technology adoption.

Keywords: participatory design, military AI, automated functions, sociotechnical systems

ROUNDTABLES

JONAH BOYER*
DAVID LAST[2]

PASTORAL TO OPERATIONAL: THE ROLE OF CHAPLAINS IN BUILDING COHESION AND MORAL RESILIENCE IN DIVERSE FORCES

*-[2]Royal Military College of Canada-Kingston

This research examines how chaplains are employed within the military forces of a multicultural democracy. It seeks to understand how policies are developed and implemented at the ground level, and to assess their effects on unit cohesion, moral resilience, and institutional effectiveness. The research investigates which policies drive the chaplaincy in the Canadian Armed Forces and how they are applied at the unit level both domestically and internationally, including contexts such as religious leader engagement. It additionally aims to understand the utility of chaplains within multinational cooperation and leadership environments, such as the multinational brigade in Latvia. The research employs a qualitative approach to analysing data drawn from primary documents, secondary sources, and academic literature, including policy documents, systematic reviews, and comparative studies. Secondary sources describing other states are compared to understand the relationship of chaplains to inner and outer, and individual and collective ministries, and how chaplains affect unit effectiveness and help address the gap between the military and society. Semi-structured interviews with subject experts will be conducted to answer factual questions about policy implementation and its effects on unit culture, military culture, and operations. Preliminary results suggest that chaplains can meaningfully improve cohesion, moral resilience, and unit effectiveness by building trust, reinforcing common values, and fostering a sense of belonging and purpose within diverse military formations. Comparing established policies across national contexts aims to inform the evolution of chaplain doctrine in ways that enhance operational effectiveness and contribute to force multiplication. Ultimately, this research seeks to demonstrate that a well-integrated chaplaincy is not merely a pastoral support function, but a strategic asset within the modern multicultural military institution.

Keywords: chaplaincy, cohesion, resilience, policy, operations

WORKING GROUP 6:
SECURITY AND DEFENCE POLICY

Chair

HERWIG JEDLAUCNIK
Austrian National Defence Academy

Co-Chair

KRISTINE ATMANTE
Baltic Defence College

TAHIR AZAD*

HYPERSONIC WEAPONS AND THE TRANSFORMATION OF STRATEGIC STABILITY IN CONTEMPORARY WARFARE

*University of Reading

The rapid proliferation of hypersonic glide vehicles and hypersonic cruise missiles is fundamentally reshaping deterrence dynamics, crisis behaviour, and escalation pathways across an increasingly multipolar security environment. This paper argues that hypersonic weapons do not merely introduce incremental improvements in speed and range but structurally alter the offence-defence balance in ways that existing military doctrines and arms control frameworks are ill-equipped to address. Critically, no operational ballistic missile defence system currently exists that can reliably intercept hypersonic weapons. Their manoeuvrability, depressed trajectories, and capacity to operate within the atmospheric grey zone between traditional ballistic and aerodynamic flight regimes defeat established intercept geometries, rendering existing defence architectures strategically redundant. Drawing on four contemporary cases, including the Russia-Ukraine war, the 2025 India-Pakistan crisis, the June 2025 Twelve-Day War, and the 2026 US/Israel-Iran conflict, the paper examines how hypersonic and multi-domain capabilities are accelerating competitive military modernisation and destabilising regional deterrence architectures. The 2026 Iran theatre is given particular attention as an empirical case of deterrence breakdown under conditions of saturation strike, absent defensive intercept capability, and acute nuclear ambiguity. Methodologically, the study combines qualitative doctrinal analysis with evidence drawn from defence reports, policy documents, and open-source intelligence. The paper concludes that without new arms control frameworks and confidence-building mechanisms specifically designed for the hypersonic era, continued proliferation will deepen strategic instability, demanding urgent adaptation of deterrence strategy, escalation management, and missile defence policy.

Keywords: hypersonic weapons, strategic stability, deterrence, multi-domain warfare, arms control, escalation, missile defence, great power competition

SUMANTA BHATTACHARYA*
BHAVNEET KAUR SACHDEV[2]

THE MILITARIZATION OF CYBERSPACE, DIGITAL AUTHORITARIANISM, AND CROSS-BORDER DATA WARFARE: RECONCEIVING COOPERATIVE DEFENCE GOVERNANCE AND NATIONAL SECURITY IN THE ERA OF ALGORITHMIC CONFLICT

*CENJOWS, [2]Suresh Gyan Vihar University

Artificial Intelligence (AI), cybersecurity, algorithmic decision-making, and networked data governance are redefining the nature of modern warfare. Geopolitical competition, in contrast to traditional conceptions of war and military deployments, is motivated by cross-border data manipulation, autonomous cyber operations against enemy states or other targets (private or public), AI-enabled disinformation, and the strategic domination over flourishing digital infrastructure across multiple nations. At the same time, digital authoritarianism has grown, as states have begun using AI for surveillance and predictive analytics of behaviors to entrench domestic control or demonstrate international strength through centralized data governance. The emerging issues further expose the continued state-centrism and technological shortcomings built into existing international legal and security structures. This study re-envisions national security with a cooperative defence governance framework framing technological innovation across international law, cyber diplomacy, and democratic accountability. It utilises a multi-dimensional analytical framework containing Cyber Power Theory, Securitization Theory, and Complex Interdependence Theory to assess data as an instrument for strategic security. Utilizing qualitative doctrinal and comparative policy analysis, the work references international legal instruments as well as national cybersecurity strategies, AI governance frameworks, and multilateral organization policy documents.

Findings: Comparative case studies of the Russia-Ukraine cyber conflict, US-China technological competition, and shifting European cybersecurity governance reveal a number of institutional, legal, and strategic trends. The results suggest diverging ineffectiveness of unilateral responses against algorithm-based cyber challenges. Limited international coordination, inconsistent digital sovereignty norms, and fragmented governance undermine collective resilience. This article proposes a multilayered governance framework built upon interoperable cybersecurity policies, responsible civic and corporate AI principles, intelligence-sharing mechanisms for attribution, cross-border data guidelines, and coordinated cyber deterrence. It concludes that winning the national security race in this age of algorithmic war will require not only technological supremacy but also new forms of transparent, collaborative, and dynamic governance.

Keywords: cyberspace, cyber welfare, digital infrastructures, cross-border manipulation, defence governance

HAFEEZ BIN ROMAINOR*

SOFT-HEDGING FOR RESILIENCE: MALAYSIA'S DEFENCE ACQUISITION IN THE AGE OF HYBRID AND MULTI-DOMAIN WARFARE

*Rabdan Academy

This paper examines how Malaysia's defence acquisition diversification functions as a soft-hedging strategy to enhance security resilience and preserve strategic autonomy amid intensifying great power competition and evolving multi-domain threats. Specifically, it asks: *To what extent does Malaysia's defence procurement diversification constitute an adaptive security policy that strengthens national resilience while maintaining strategic flexibility?* The study is theoretically grounded in Kuik's (2008) hedging theory, complemented by the concepts of strategic autonomy and security resilience to explain how middle powers manage geopolitical uncertainty without aligning exclusively with any major power.

Recent conflicts in the Indo-Pacific, Ukraine, and the Middle East have underscored the growing importance of supply-chain resilience, unmanned systems, and cyber-enabled operations. These developments expose the vulnerabilities associated with excessive dependence on a single defence supplier or strategic partner. The recent revocation of Malaysia's missile procurement from Norway further illustrates the risks of procurement dependency and reinforces the need for a diversified acquisition strategy.

The study adopts a qualitative case study approach based on document analysis of Malaysia's defence procurement patterns, official policy documents, government statements, and recent regional security developments. It analyses how procurement decisions reflect Malaysia's broader soft-hedging strategy, consistent with ASEAN's principle of non-interference and Malaysia's longstanding non-aligned foreign policy.

The paper argues that defence acquisition diversification serves as an adaptive security policy by reducing strategic dependence, expanding access to diverse military technologies, and increasing policymakers' strategic options during geopolitical crises. Although diversification presents challenges in interoperability, logistics, and sustainment, it remains a pragmatic approach for enhancing Malaysia's security resilience while preserving strategic autonomy in an increasingly contested regional security environment.

Keywords: Malaysia, soft-hedging, defence acquisition, ASEAN

MARLENA BLICHARZ*

ATTITUDES TOWARDS NUCLEAR WEAPONS AND NUCLEAR ENERGY AMONG YOUNG PEOPLE IN PL AND KOR. ABSTRACT PROPOSAL

*War Studies University

This study examines attitudes toward nuclear weapons and nuclear energy among young people in Poland and South Korea, focusing on how historical experience, security concerns, energy policy, and generational identity shape public opinion. Although both countries are strategically positioned near regional security threats and rely to varying degrees on nuclear energy, their historical trajectories and geopolitical environments differ significantly. These differences provide a valuable comparative framework for understanding contemporary youth perspectives on nuclear-related issues.

The research investigates whether support for civilian nuclear energy correlates with acceptance of nuclear deterrence and military nuclearization. It also explores how perceptions of national security, climate change, technological progress, and trust in government influence these attitudes. In Poland, debates surrounding energy transition, dependence on external energy sources, and regional insecurity linked to Russia have intensified public discussion on nuclear policy. In South Korea, ongoing tensions with North Korea and the country's advanced nuclear energy infrastructure create a distinct political and social context for young citizens.

The analysis aims to identify similarities and divergences in generational attitudes, particularly regarding the perceived legitimacy of nuclear deterrence versus the environmental and economic benefits of nuclear power.

The research is an introduction to broader discussions in international relations, energy politics, and youth political culture by highlighting how younger generations in democratic societies negotiate the relationship between security and sustainability. It also seeks to provide insight into the future public legitimacy of nuclear policy in Europe and East Asia.

Keywords: security, nuclear energy, nuclear deterrence, Korean Peninsula, Poland

JEIMY CANO*

THE EVOLUTION OF STATE CYBER DEFENCES IN THE 21ST CENTURY: FROM ROBUST DEFENCES TO ANTIFRAGILE DEFENCES

*Universidad de los Andes

In an increasingly nonlinear, fast-paced, volatile, and interconnected environment, states need to update their perspectives and doctrines regarding cybersecurity and cyberdefense. In this regard, this paper analyzes the conceptual and operational evolution of nations' cyberdefense strategies, ranging from robust defense postures focused on perimeter prevention, through resilient models oriented toward recovery, to antifragile configurations that view each incident as an opportunity for learning and systemic strengthening. This study adopts a qualitative, analytical-descriptive approach, integrating theoretical frameworks from resilience engineering (Park et al. 2013), the theory of antifragility (Taleb 2012), weak signal analysis applied to threat anticipation (Hiltunen 2008), and chaos engineering applied to information technology systems (Tseitlin 2013). The article identifies three defensive postures distinguished by their design philosophy, their relationship to failure, and success criteria, as well as analyzes real-world application cases in Estonia (2007), the United States (2008), Israel (active defense model), Netflix (Simian Army), and Ukraine (2022). A four-phase transition strategy is proposed to enable states to progressively evolve from a robust posture toward an antifragile one, with defined time horizons and some maturity criteria. The main contribution of this study lies in the articulation of an integrative conceptual framework that allows decision-makers – particularly states and commanders of joint cyber commands – to understand the advantages, limitations, and conditions of applicability of each defensive posture, and to design strategic transformation pathways tailored to their institutional capabilities and the current threat environment.

Keywords: state cyber defense, antifragility, cyber resilience, robust defense, chaos engineering

ADEWUNMI JAMES FALODE*

TERRORISM, BANDITRY, AND CRIMINALITY IN NIGERIA: A STRATEGIC ANALYSIS OF THE CRIME-TERROR NEXUS

*Lagos State University

This paper presents a strategic analysis of the evolving dynamics and interactions between terrorist organizations and criminal networks, including armed bandits, kidnappers, and arms smugglers, in Nigeria. The study adopts a qualitative research design that combines a systematic literature review with content analysis of secondary sources, including security reports, government and multilateral documents, and media coverage, supplemented by case studies of prominent terrorist groups like Boko Haram, the Islamic State West Africa Province (ISWAP), and armed banditry networks in the Northwest, such as Bello Turji's and Halilu Sububu's gangs. Theoretically, the paper is anchored in the Crime-Terror Nexus framework, particularly Makarenko's crime-terror continuum, which conceptualizes the relationship between ideologically motivated and profit-driven violence as a spectrum of interaction rather than a fixed dichotomy. Applying this framework, the study argues that significant operational convergence exists among these actors at both tactical and strategic levels within Nigeria's broader security environment and the West African region. Rather than operating as isolated phenomena, the study shows that terrorism and organized criminality increasingly overlap in financing, logistics, territorial control, and recruitment. The analysis demonstrates that criminal activities such as cattle rustling, kidnapping, illicit arms trafficking, and banditry mutually reinforce terrorist operations, producing hybrid security threats that complicate the state's conventional counter-insurgency and counter-terrorism responses. This convergence blurs the boundaries between ideologically driven violence and profit-motivated crime, creating adaptive and resilient networks of violence that challenge state authority. The paper further argues that this nexus is reshaping the conflict architecture in Nigeria and contributing to broader regional insecurity across the Sahel and Lake Chad Basin. It concludes that countering these hybrid threats requires a proactive and synchronized security response that integrates counter-insurgency (COIN), counter-terrorism, intelligence-led policing, and regional cooperation, going beyond fragmented and ineffective institutional and statist approaches.

Keywords: terrorism, Nigeria, crime-terror nexus, strategy, COIN

FRANCESCO FIMIANI*

DRONES, DETERRENCE, AND THE BALTIC GAP: THE STRATEGIC ADVANTAGE OF DOMESTIC DRONE PRODUCTION IN THE CASE OF ESTONIA

*Hertie School

How can small frontline states strengthen deterrence amid growing geopolitical instability and uncertain alliance commitments? This thesis examines Estonia as a case study to assess how domestically produced unmanned aerial vehicles (UAVs) can enhance national defense and delay adversary advances during the critical window before NATO reinforcement. While drones have transformed modern warfare, their strategic application by technologically advanced yet manpower-constrained states remains under-theorized in existing defense literature. This study argues that Estonia's world-leading cybersecurity infrastructure, vibrant defense-tech ecosystem, and evolving military doctrine uniquely position it to integrate drones into a national deterrence posture capable of exploiting Russian operational vulnerabilities. Drawing on expert interviews with defense analysts and practitioners, QGIS-based geospatial modelling of critical infrastructure and population centres, and open-source military data, the research models how UAVs could be deployed along Estonia's eastern border to disrupt and delay Russian forces during the so-called "NATO time gap". Key findings indicate that public-private partnerships in drone development offer a scalable, cost-effective force multiplier for small allies but will not substitute the necessity of establishing air superiority. The thesis contributes to emerging debates on asymmetric deterrence, defense technology diffusion within alliance frameworks, and the feasibility of greater European strategic autonomy as transatlantic security commitments face new uncertainties. Its conclusions offer actionable insights for Baltic defense planners seeking to leverage indigenous technological advantages in an era of constrained resources and evolving threats.

Keywords: UAVs, Baltic defense, deterrence, drones, NATO

MARTA GĘBSKA*

PERCEPTION OF THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES – RESULTS OF OWN RESEARCH IN THE US

*War Studies University

The study will focus on the perception of the strategy in the context of its implementation. A survey conducted among students, employees, and residents of Florida will focus on the perceived achievement of the objectives of the National Security Strategy (NSS 2025). Thus, the study will address not only opinions about the document but also an assessment of the policies pursued by the administration following its adoption. This is consistent with the approach used in policy implementation studies.

The national security strategy is a document that sets the direction for the government's actions, but its significance is not limited to the content of its provisions. From the perspective of political science and security studies, the process of implementing the strategy and the public's assessment of the effectiveness of the measures taken are of key importance. For this reason, the focus of this study is not on respondents' level of familiarity with the document, but rather on their perception of the extent to which the US government has implemented its main objectives since its adoption. This approach aligns with the field of research on policy implementation and public opinion surveys, which analyze public assessments of the actions of public institutions rather than merely familiarity with policy documents. In political science, in turn, the perceived effectiveness of the administration, trust in institutions, evaluations of the implementation of government programs, and assessments of reforms are frequently analyzed.

The study will focus on security issues at the national and international levels.

Keywords: strategy, the United States, security, perception

CAROLA GRITELLA*
FABIO BIONDI[2], GUERRINO MAZZAROLO[3]

HYBRID ATTACKS AGAINST HEALTHCARE CRITICAL INFRASTRUCTURES (HCI): RESILIENCE AND DEFENSIVE OPERATIONS

*University of Turin, [2]Italian Cyber Command, [3]University of Maastricht

Cyberattacks against healthcare critical infrastructure (HCI) have surged across the EU and NATO, with the European Union Agency for Cybersecurity (ENISA) ranking the health sector among the top five targets for state-aligned actors.

Adversaries strategically deploy Tactics, Techniques, and Procedures (TTPs) to destabilize societies. By compromising patient data, disrupting hospital admissions, and delaying critical care, these attacks aim to erode public trust in governance creating fertile ground for disinformation that could escalate into protests and physical sabotage.

This threat is amplified by the convergence of offensive Artificial Intelligence (AI) and systemic HCI vulnerabilities, both increasingly exploited for hostile purposes. Passive resilience is no longer sufficient to withstand the scale, sophistication, and speed of attacks, combined with the diverse and diffuse tactics employed in hybrid warfare. This paper explores the exposure of HCI to dynamic AI-driven cyber threats and hybrid warfare arguing for a paradigm shift from compliance-based HCI protection toward proactive cyber defense operations that integrate the physical dimension.

Drawing on open-source incident databases and foresight-based scenario analysis, the paper investigates how such threats could compromise societal stability. To address these risks, it outlines a multidisciplinary resilience model that considers technical, strategic, and cooperative defense measures offering a foundational framework for proactive cyber operations that contributes to the defense of the public health sector.

Keywords: healthcare critical infrastructures, resilience, defensive operations, hybrid warfare

OĞUZHAN GÜNGÖR*
AYŞEGÜL BOSTAN[2]

TÜRKIYE'S INDISPENSABLE STRATEGIC ROLE IN THE EUROPEAN SECURITY FRAMEWORK

*-[2]Turkish National Defence University

Recent conflicts, particularly the war in Ukraine and the Second Karabakh War, demonstrate that contemporary warfare is undergoing technological and strategic transformation. The vulnerability of critical infrastructure and military platforms, the growing importance of network-centric warfare, the expanding role of unmanned systems, and ammunition production and consumption are central concerns for European security. At the same time, policy divergences between the United States and its European allies have intensified debates over Europe's strategic autonomy and its capacity to assume greater defence responsibility.

Against this background, European defence initiatives, including the EU Strategic Compass and programmes strengthening defence readiness and industrial capacity, seek to improve cyber resilience, counter hybrid threats, protect critical infrastructure, and enhance military capabilities. Their effectiveness, however, also depends on cooperation with strategically important non-EU allies.

This study asks: To what extent, and through which military, geopolitical, diplomatic, and defence-industrial mechanisms, does Türkiye contribute to Europe's evolving security architecture? It argues that Türkiye's geographical position, NATO membership, operational capabilities, expanding defence industry, and strategically autonomous policies make it an indispensable, though institutionally contested, component of European security.

Methodologically, the study employs a qualitative case study approach supported by descriptive quantitative data. It combines analysis of EU, NATO, and Turkish strategic documents with case studies of Türkiye's role in Ukraine and the Second Karabakh War. Defence expenditure, military capacity, defence-industrial production, unmanned systems, and NATO contributions complement the qualitative analysis. The theoretical framework draws on strategic autonomy, security interdependence, and middle-power agency.

The findings indicate that Türkiye's contributions extend beyond conventional military deterrence. Its role in the Black Sea Grain Initiative, mediation efforts, implementation of the Montreux Convention, operational experience, and defence-industrial capabilities demonstrate its capacity to act as a stabilising, balancing, and agenda-shaping actor. The study concludes that credible European security ultimately requires structured and pragmatic cooperation with Türkiye.

Keywords: European security, strategic autonomy, warfare transformation, Türkiye, international security

SIDDHANT HIRA*

BUILDING COGNITIVE RESILIENCE IN INDIA'S THREAT LANDSCAPE

*NatStrat

The global security landscape is increasingly defined by 'permanent competition', where the distinction between war and peace is blurred by persistent adversarial operations in the cognitive domain. For India, this shift is not merely a technical challenge but a strategic imperative as the country faces sophisticated cognitive attacks from its primary adversaries, China and Pakistan.

This paper examines the necessity of elevating cognitive security from a whole-of-government to a whole-of-society approach. Cyber resilience is the need of the hour today, tomorrow, and every day. The path to cyber resilience begins with cyber literacy, followed by cyber awareness; it is a broad roadmap to secure the population. Anchored in an analysis of India's evolving digital dependence and the vulnerabilities introduced by cyber illiteracy, the study argues that developing societal cyber resilience is an imperative. Methodologically, the article employs a qualitative analysis of regional threat perceptions and adversarial influence operations that treat the Indian 'home-front' as a contested domain. It explores how adversaries leverage cognitive illiteracy to trigger polarisation and undermine societal cohesion.

The paper's key contribution lies in proposing a framework for a 'vulnerability-resilience nexus'. It argues that for New Delhi to secure its critical infrastructure and democratic fabric, it must transition toward a proactive strategic posture that builds sustained cognitive defence. This is also an opportune moment for India to learn from Europe about the Russian cognitive threat and for Europe to learn from India about the Chinese cognitive threat, and to develop countermeasures. Integrating cognitive security into the National Security Strategy is essential for regional stability and for resisting the protracted, grey-zone pressures characteristic of 21st-century statecraft.

Keywords: cognitive resilience, cyber resilience, cyber awareness, cyber illiteracy, societal resilience

MARTINS DA COSTA HUGO BRAS*

CRISIS OF MULTILATERALISM, MODERN UN PEACEKEEPING OPERATIONS, AND BRAZIL'S STRATEGIC ROLE

*Brazilian Army Command and General Staff School (ECEME)

The current context is marked by political fragmentation and legitimacy crises in international organizations, challenging multilateralism's capacity to maintain international peace and security. Today, there is an urgent need for critical reflection on how institutionalized multilateralism can reinvent itself to remain relevant, efficient, and effective. Peace operations are the United Nations' most visible tool to manage conflicts. Referred to as "multilateralism in action" by the UN Secretary-General, António Guterres, these missions are directly affected by this turning point, where the crisis of multilateralism intertwines with the need to strengthen its resilience. In an increasingly multipolar world, the foundational consensus sustaining blue-helmet deployments faces unprecedented strain. Brazil is in a privileged position to engage in this debate due to its unique trajectory, active contribution to consensus-building, and long-standing deployment of military personnel to diverse missions. The theoretical and analytical framework of this paper addresses the ongoing crisis not as a pathology, but as the very 'matrix' of multilateralism's transformative resilience, as posited by Guilbaud, Petiteville, and Ramel. Methodologically, it employs a qualitative document analysis to examine the direct correlation between political fragmentation within decision-making bodies and the practical challenges encountered by troops on the ground. To map this link, the research triangulates UN Security Council resolutions, UN Secretariat reports, and UN budget reports collected via the UN Digital Library. Concurrently, to understand how Brazil's defense policy ensures international standing amidst these uncertainties, the paper draws on Amitav Acharya's norm diffusion analysis, the Foreign Policy Analysis literature, and the French socio-historical approach. Empirically, it assesses Brazil's normative and doctrinal positions regarding the structuring and renewal of peacekeeping missions by analyzing the statements and discourses delivered by the Brazilian delegation during the yearly opening debates of the UN Special Committee on Peacekeeping Operations (C-34).

Keywords: crisis of multilateralism, UN, peacekeeping operations, Brazil, international peace and security

MISAKO ISHIKAWA*

THE GEOPOLITICS OF WORDS: RECOGNITION, DIPLOMATIC TRUST, AND CONFLICT RESOLUTION – LESSONS FROM YUGOSLAVIA (1990S TO THE EARLY 21ST CENTURY)

*Shitennoji High School

This paper re-examines military and diplomatic postures in today's conflict environment. Drawing on Henry Kissinger's realism and Thomas Schelling's bargaining theory, it proposes a framework that combines rational signalling – emphasising predictability – with negotiatory flexibility. This is analysed through the political processes of the Kosovo conflict.

In contemporary politics, Francis Fukuyama's concepts of recognition and identity politicisation often drive decision-making. These dynamics were evident during Yugoslavia's dissolution. In the 1990s, political elites mobilised ethnic identities amid economic crisis and the collapse of communism. Nationalist rhetoric deepened distrust, eroding "constructive ambiguity" and necessitating prolonged intervention in Bosnia and Kosovo.

The paper focuses on the "geopolitics of words", where public statements act as irreversible commitments that constrain flexibility. Schelling's "bargaining game" views conflict as strategic interaction rather than mere emotional antagonism. Clear signalling and rational firmness reduce misperceptions and escalation risks.

Ultimately, external predictability is vital. A state acting as a "negotiable contractual actor" strengthens deterrence and dialogue. The divergent paths of Croatia, Bosnia, and Kosovo suggest that institutional design and predictability are decisive for stability. Balancing these elements allows for rational policy even in identity-driven crises.

Keywords: Yugoslav politics, geopolitics, military strategy, negotiation

EMMANUEL KARAGIANNIS*

DIVERGENT DEFENCE TRAJECTORIES: A COMPARATIVE ANALYSIS OF GREEK AND CYPRIOT MILITARY REFORMS

*King's College London

Greece and Cyprus are pursuing parallel, yet distinct defence reforms shaped by evolving regional security dynamics, technological change, and shifting strategic alignments. This paper conducts a comparative analysis across four dimensions: conscription, budget, defence industry, and infrastructure. Greece's "Agenda 2030" introduces a significant restructuring of its conscription system, restricting compulsory service to the Army while transitioning the Navy and Air Force to fully professional forces. Enhanced training and increased compensation are designed to improve readiness and attract specialised personnel. Cyprus, by contrast, retains its traditional conscription model, focusing on targeted professionalisation and international training partnerships within the existing framework. Divergence is also evident in defence spending. Greece is investing heavily in advanced platforms – including F-35s, upgraded F-16s, Black Hawks, and FDI-HN frigates – alongside the "Achilles Shield" multi-layered defence system. Cyprus' more modest budget prioritises the replacement of legacy Russian systems, cyber capabilities, and surveillance assets to strengthen asymmetric defence. Both states aim to expand their domestic defence industries, though with different levels of ambition and institutional capacity. Infrastructure reforms further underscore their divergent trajectories: Greece is consolidating bases and restructuring command regions, whereas Cyprus is upgrading key air and naval installations to enhance interoperability and deterrence. The paper offers a systematic comparison of these reform pathways, assessing their strategic drivers, institutional implications, and potential impact on regional security.

Keywords: Greece, Cyprus, defence reforms, conscription, defence industry

SUSAN KHAZAELI*

FROM GRAY ZONE TO CONTINUOUS CONFLICT: RECONFIGURING DETERRENCE IN HYBRID WARFARE

*Development Research Defence Canada

This paper examines how state and non-state actors in the Middle East reshape hybrid-threat activity under conditions of regional competition and episodic escalation. Drawing on a historically grounded analysis of conflict and informed by research on nuclear proliferation and deterrence, I argue that prevailing “gray zone” frameworks inadequately capture how conflict is operationalized in the region.

Regional actors increasingly treat conflict as a continuous and integrated spectrum, synchronizing military, political, economic, and informational tools. The analysis highlights three dynamics: the growing centrality of proxy and partner-enabled operations; the use of calibrated escalation to manage risk; and the expansion of competition into economic and geographic domains, including critical infrastructure and maritime spaces.

Focusing on patterns observable across Iranian, Israeli, and Gulf approaches, deterrence is not simply eroding but being reconfigured under conditions of strategic uncertainty. Actors are shifting toward strategies of attrition and punishment that prioritize endurance, cost imposition, and strategic signaling over decisive outcomes. This shift reflects limits in traditional deterrence models, particularly under conditions of nuclear latency, ambiguity, and asymmetric capability development. This reflects a broader transformation in which hybrid activity becomes not a prelude to war but a persistent operating logic that extends into periods of open conflict.

The paper concludes that understanding hybrid threats in the Middle East requires moving beyond threshold-based models toward frameworks that account for continuous competition, networked actors, and contested escalation. By integrating insights from deterrence theory and historical analysis, these findings have implications for strategy development, force design, and defence policy in increasingly complex multi-domain environments.

KLEMEN KOCJANCIC*

FROM TERRITORIAL DEFENCE TO TERRITORIAL FORCE: A TRANSFORMATION OF MILITARY STRATEGIC RESERVE FORCES IN SLOVENIA

*Ministry of Defence of the Republic of Slovenia

The development of military strategic (reserve) forces in Slovenia represents a unique case of military transformation in Central and Southeastern Europe. Continuing the tradition of partisan units from the Second World War, during the Cold War, a Yugoslav concept of General People's Defence and Social Self-Protection established Territorial Defence (TD) in each of the Yugoslav constituent republics and autonomous provinces. Although formally part of armed forces, TD became a decentralized reserve-based force, which was then a key instrument of securing national sovereignty and state-building during the Slovenian War of Independence in 1991.

After the TD were reformed into a regular armed force of Slovenia (Slovenian Armed Forces, SAF), through the process of transformation, the role of reserve military forces diminished. Only with the Russian invasion of Ukraine in 2022 did the necessity of a military strategic force become evident, resulting in the establishment of the Territorial Force Command.

This paper examines the historical evolution of the Slovenian Territorial Defence from its establishment in 1968 through the period of democratic transition, the 1991 independence process, and its subsequent integration into the defence structures of the independent Republic of Slovenia, culminating in the current form of the Territorial Force.

Using historical institutionalism and qualitative analysis of archival sources, legal documents, and contemporary literature, the paper explores the continuity, discontinuity, and reinvention of territorial defence principles in Slovenia's modern defence system when faced with internal and external influences and explains how critical security shocks and strategic goals interact with inherited defence institutions to shape military reserve reforms. The study contributes to broader discussions on reserve forces, national resilience, and the adaptation of small-state defence models in changing security environments.

Keywords: Slovenian Armed Forces, military reserves, strategic reserve, territorial defence, territorial force

IVANA KOVAČEVIĆ BEKIĆ*
TATJANA ŠOLAJA[2]

INFORMATION WARFARE AND NATIONAL SECURITY CHALLENGES OF SMALL STATES: STRATEGIC VULNERABILITIES AND RESILIENCE IN THE DIGITAL AGE

*-[2]Ministry of Defence of the Republic of Croatia

The contemporary security environment is increasingly characterized by hybrid threats and information warfare, where digital platforms, strategic narratives, and disinformation campaigns are employed to influence political processes, public perception, and national stability. Small states are particularly vulnerable to such activities due to limited institutional capacities, smaller media environments, and their reliance on international security frameworks.

This paper examines the impact of information warfare on the national security of small states, with particular emphasis on the challenges posed by disinformation, cognitive warfare, and strategic influence operations in the digital domain. The research explores how hybrid information threats affect political resilience, public trust, and strategic decision-making processes within small democratic societies.

The study is based on a qualitative methodology that includes a review of relevant academic literature, an analysis of strategic documents issued by NATO and the European Union, and a case study approach. As an empirical example, the paper examines a small NATO and European Union member state in Southeast Europe in order to identify vulnerabilities and resilience mechanisms relevant to contemporary information threats.

The findings indicate that small states remain highly exposed to external information influences due to limited strategic communication capacities and increasing societal polarization. However, international integration, institutional cooperation, media literacy, and the development of national strategic communication systems can significantly contribute to strengthening societal and information resilience and enhancing national security.

The paper contributes to contemporary discussions on hybrid warfare and security policy by highlighting the importance of societal and information resilience as key components of defence and security strategies for small states operating in the contemporary security environment.

Keywords: information warfare, national security, small states, hybrid threats, disinformation, resilience, strategic communication

AGUSTIN MACIEL*

JAPAN'S COUNTERSTRIKE CAPABILITY: PUSHING THE LIMITS OF A DEFENSE-ORIENTED POLICY

*Rabdan Academy

This analysis explores the most significant change in Japan's defense policy since the end of World War II; the most remarkable proposition is to acquire a counterstrike capability, consisting of long-range cruise missiles to strike deep into a potential adversary's territory. Contrary to arguments pointing out these plans represent an "unprecedented" transformation of Japan's defense policy since 1946, they are rather the logical consequence of a gradual, but significant, change, that has been occurring since at least a couple of decades. These recent proposals are explored within the wider debate about whether Japan should continue pursuing a pacifist posture, or to adopt a more assertive stance in response to a more threatening international environment.

Regarding methodology, this study draws upon the realist theory as its primary analytical lens. Applying this framework allows for an interpretation of Japan's counterstrike policy as a strategic response to perceived threats and changing power dynamics in East Asia. This analysis adopts a qualitative, case-study approach focused on Japan's evolving defense policy. It does not aim to test realism against alternative theories but instead uses the realist perspective as an interpretative framework to explain Japan's policy choices. The study relies on primary sources including Japan government's documents and official statements, in addition to academic and policy literature such as scholarly reports from think tanks and peer-reviewed articles and news media from Japan and outlets in other countries. This analysis is based, first, in the contextualization of Japan's decision in the broader East Asia security and international environments; second, in the application of realist concepts explaining Japan's adoption of counterstrike capabilities as a rational, survival-oriented, response within an anarchic system aiming at addressing regional threats; and third, in the assessment of the implications of this realist orientation in Japan's regional role, its alliance with the United States, and potential escalation dynamics in East Asia.

Keywords: Japan, defense policy, counterstrike capability, US Alliance, PME

MAREKS MATISONS*

THE CASE FOR HOMELAND OVER DOMESTIC: A LINGUISTIC AND CULTURAL ARGUMENT

*NAF Latvia, National Guard

This study grounds its framework in the Copenhagen School's concept of societal security (Wæver et al., 1993; Buzan et al., 1998), which decouples security from state machinery. While orthodox paradigms prioritize state sovereignty, societal security elevates a community's collective "we-identity" as the primary referent object. Here, the existential threat is not physical conquest, but the disruption of shared values, culture, and identity that sustain social coherence.

Applying this lens to civil-military cooperation (CIMIC) exposes a core flaw in NATO doctrine. Expeditionary operations under AJP-3.19 treat the local civil environment as an operational variable to manage, with the allied force as the referent object.

Homeland defense inverts this dynamic. The civilian population becomes the primary referent object. In frontline nations reliant on total defense, citizens are simultaneously the entity being defended and the primary agent providing that security. This is not an operational shift that can be managed by downsizing expeditionary CIMIC templates – it is a fundamental difference in kind.

Consequently, AJP-3.19 Edition B's assumptions collapse when the military force and the secured society are identical. The doctrine's shortfall is structural, not an editorial omission easily patched in future revisions.

This gap is felt most acutely at the operational-tactical interface. Territorial defense forces, such as Latvia's 1st Riga Brigade, act as classic societal security institutions: they project kinetic deterrence while reinforcing community cohesion. That practitioners within these frontline units identify this doctrinal blind spot is a direct result of their position at the intersection of local society and allied military doctrine.

Keywords: CIMIC, domestic CIMIC, Homeland CIMIC, AJP-3.19, civil-military cooperation, host nation support, resilience, defence innovation, Latvia, Zemessardze, NATO doctrine

NICOLE NEVES*

THE REGIONALIZATION OF PEACE OPERATIONS AND THE RECONFIGURATION OF SECURITY GOVERNANCE IN AFRICA: A HISTORICAL-INSTITUTIONALIST FRAMEWORK

*Brazilian Army Command and General Staff College (ECEME)

The relative retrenchment of United Nations peacekeeping operations and the growing regionalization of conflict responses in Africa have significantly transformed multinational peace and security arrangements. Over the past two decades, the African Union (AU) and the African Peace and Security Architecture (APSA) have assumed a central role in crisis management, stabilization, and peace support operations, reshaping how responsibilities and strategic authority are distributed between global and regional actors. This article seeks to address the following question: How can the regionalization of peace operations be conceptualized as a process of institutional adaptation and strategic reconfiguration within African security governance?

The analysis argues that this process should not be understood merely as a functional transfer of responsibilities from the United Nations to the African Union. Rather, it constitutes a broader process of institutional reconfiguration, in which regional operational leadership expands while mandate authorization, financing, and long-term strategic coordination remain embedded in multilevel governance arrangements. Drawing on historical institutionalism as its central analytical framework, the article mobilizes the concepts of path dependence, gradual institutional change, and institutional adaptation to explain how the AU's security role has evolved incrementally within the APSA framework. It also engages with the literature on global security governance, African regionalism, and postcolonial critiques of international order to propose an integrated analytical model for contemporary multinational peace operations.

Keywords: security governance, peace operations, historical institutionalism, African Union, regionalization

MILENA PALCZEWSKA*

FROM CLIMATE CRISIS TO HUMAN MOBILITY: SECURITY IMPLICATIONS OF CLIMATE-INDUCED MIGRATION

*War Studies University

Climate-induced migration has become one of the most significant non-military security challenges of the twenty-first century. Rising sea levels, prolonged droughts, desertification, and extreme weather events increasingly contribute to human displacement and cross-border mobility, generating humanitarian, political, economic, and social consequences that challenge national and international security systems.

This presentation will examine how climate-induced migration reshapes contemporary security paradigms and tests the capacity of existing governance mechanisms to respond to environmentally driven population movements. It asks whether current legal and institutional frameworks adequately address the security implications of climate-related migration and how these processes influence regional stability and international cooperation.

The analysis is grounded in the theoretical perspectives of securitization theory and human security, complemented by insights from migration studies and international relations. This interdisciplinary framework enables an examination of the links between environmental degradation, forced mobility, resource competition, and evolving security dynamics.

Methodologically, presentation employs a qualitative research design based on comparative case study analysis and document analysis. The study examines selected climate-vulnerable regions experiencing significant displacement, drawing on international reports, policy documents, legal instruments, and academic literature published by international organizations and leading research institutions. The analytical approach combines thematic analysis with comparative assessment to identify recurring patterns in the relationship between climate change, migration, and security outcomes.

The presentation argues that climate-induced migration should be understood not only as a humanitarian concern but also as a multidimensional security issue requiring integrated governance frameworks. The findings contribute to ongoing debates on the securitization of climate change and highlight the need for adaptive, preventive, and internationally coordinated policy responses to climate-driven human mobility.

Keywords: climate-induced migration, human security, environmental displacement

DUMITRU-CATALIN VASILE*

DIGITAL SOVEREIGNTY AND DEMOCRATIC LEGITIMACY IN AI-ENABLED DEFENCE GOVERNANCE

*National School of Political and Administrative Studies

The rapid proliferation of Artificial Intelligence (AI) has fundamentally disrupted traditional notions of state authority, necessitating a critical re-evaluation of the nexus between technological autonomy and democratic governance in the defense sector. Within this context, the objectives of the study are to investigate the evolving relationship between AI governance and institutional legitimacy under the framework of digital sovereignty, specifically identifying the challenges defense policymakers face in balancing operational innovation with public trust. The research methods used follow a qualitative approach, combining a comparative analysis of current EU and NATO AI regulations with case studies of institutional AI implementation in security contexts. Data was gathered from diverse secondary sources, including defense policy frameworks, ethical guidelines, and scholarly debates on digital governance. The results indicate that while AI enhances administrative and operational efficiency, a persistent 'transparency gap' undermines institutional accountability, underscoring the significant threat posed by the lack of clear legal frameworks for algorithmic responsibility to democratic oversight. The study's implications emphasize the urgent need for a 'human-in-the-loop' governance model, suggesting that for AI to be successfully integrated into defense structures, legal frameworks must prioritize explainability and ethical alignment to safeguard institutional legitimacy in an increasingly automated age.

Keywords: artificial intelligence, AI Governance, digital sovereignty, defense innovation, military ethics, algorithmic accountability

LUISA VAZ*
GUSTAVO SIMÕES[2]

AN ANALYSIS OF THE LITERATURE ON THE MILITARIZATION AND SECURITIZATION OF BRAZIL'S MIGRATION AGENDA

*-[2]Escola de Comando e Estado-Maior do Exército

The social, economic, and political crisis experienced in Venezuela since 2016 has forced more than 7 million Venezuelans to seek other destinations. In 2018, due to public health concerns and pressure on public services on the country's northern border, Brazil created Operation *Acolhida*, a humanitarian response aimed at providing care to Venezuelan refugees and migrants, as well as offering voluntary, safe, and free relocation of these individuals from Roraima's municipalities to other cities in Brazil. The operation works in synergy with the Federal Government, the Armed Forces, and international organizations, totalling more than 100 institutions.

The Brazilian government's response to this situation, particularly regarding the use of military personnel in Operation *Acolhida*, has generated considerable criticism and debate, including articles and other works that use concepts such as "militarization" and "securitization" of Brazil's migration agenda. Therefore, the question guiding this article is: "How does Brazilian academic literature use the concepts of "militarization" and "securitization" when addressing Brazilian migration governance in light of the Venezuelan issue?" This paper aims to present and discuss these two concepts and their use in the context of Operation *Acolhida*. The hypothesis of this paper is that much of the literature displays considerable conceptual flexibility when using terms such as "securitization" and "militarization".

The strategy used was the use of Boolean operators, which are logical commands used to refine database searches, allowing the combination or exclusion of terms. The operators used were "AND" (to include both terms) and "OR" (to include at least one of the terms), with the following keyword combinations: 1) "*Operação Acolhida*"; 2) "*Operação Acolhida* AND Militarization"; 3) "*Operação Acolhida* AND Securitization"; and, 4) "*Operação Acolhida* AND Militarized". Finally, it is hoped that this work will contribute to Migration Studies, enabling an understanding of the political, social, economic, and military implications of this process.

Keywords: armed forces; Brazil; militarization; Operation Acolhida; securitization

KATERINA VELJANOVSKA BLAZHEVSKA*

GEOPOLITICAL TRANSFORMATIONS, STRATEGIC DELIBERATION AND DEFENCE ADAPTATION: REASSESSING STRATEGIC NORMS FOR CONTEMPORARY SECURITY CHALLENGES

*MIT University Skopje

The contemporary security environment is shaped by profound geopolitical transformations driven by armed conflicts, strategic competition among major powers, hybrid threats, technological disruption, and increasing uncertainty. These developments challenge established strategic assumptions and require continuous adaptation of defence policies, security frameworks, and decision-making processes. Consequently, the reassessment of strategic norms has become essential for addressing emerging security challenges.

This paper examines the relationship between geopolitical transformations, strategic deliberation, and defence adaptation through an interdisciplinary framework integrating contemporary security studies, geopolitical analysis, constructivist approaches to normative change, and deliberative democracy theory. It argues that deliberative processes play a central role in interpreting, contesting, and reshaping strategic norms. Particular attention is given to higher education as a deliberative space where future security professionals develop strategic thinking and competencies that support adaptive defence and security decision-making.

Methodologically, the paper employs an empirical mixed-methods research design that combines a pretest and post-test survey with moderated deliberative discussion. The study was conducted among an international cohort of university students participating in a European academic programme. Data were collected through structured Likert-scale questionnaires administered before and after a lecture on geopolitical transformations and strategic deliberation. Quantitative findings are complemented by qualitative analysis of participants' deliberative reflections to examine changes in perceptions of geopolitical threats, strategic norms, democratic resilience, and adaptive security governance.

The findings indicate that deliberative engagement strengthens strategic thinking, encourages the critical reassessment of strategic norms, and supports competencies for adaptive decision-making in complex security environments. By combining geopolitical analysis with empirical evidence from deliberative educational practice, the paper contributes to current debates on defence adaptation and strategic resilience, highlighting the role of deliberative learning in strengthening preparedness for contemporary security challenges.

Keywords: geopolitics, strategic deliberation, defence adaptation, security governance, defence innovation

WORKING GROUP 7:
ARMED FORCES AND SOCIETY

Chair

RENE MOELKER
Netherlands Defence Academy

Co-Chairs

ELERI LILLEMÄE
Estonian Military Academy and University of Tartu

KRISTIN LJUNGKVIST
Swedish Defence University

EYAL BEN-ARI*

MASS AND SOPHISTICATION: ISRAEL'S RESERVE FORCES AS A TEMPLATE FOR TWENTY-FIRST-CENTURY MILITARY INNOVATION

*Jerusalem Institute for Strategy and Security

Israel's reserve forces have long been understood as a mechanism of strategic mass. The war waged since October 2023 demonstrates that the IDF's reserve component is also one of the most sophisticated engines of military innovation in contemporary warfare, and that this innovative capacity is structurally generated rather than incidental.

The concept of 'dual capital' explains this phenomenon. Israeli reservists simultaneously carry two distinct but mutually reinforcing forms of capital: military capital, accumulated through conscription and reserve cycles – embodied tactical knowledge, unit cohesion, and operational judgment – and civilian capital, the professional expertise, social networks, and technical literacy developed in one of the world's most concentrated knowledge economies. The interaction of these two forms, not their simple addition, is the source of the reserve force's distinctive innovative power.

In the war, this dual capital structure produced bottom-up doctrinal transformation at remarkable speed: commercial drones repurposed into precision reconnaissance assets; AI-driven intelligence hubs built from civilian data science expertise; shadow logistics systems outpacing formal military supply chains; 3D-printed components manufactured in forward staging areas; and autonomous platforms improvised from commercial robotics. These were not workarounds – they were structural innovations emerging from a force whose civilian and military competencies are designed to reinforce each other.

We term this hybrid the 'Neoliberal Militia': a mass-army form achieving post-Fordist operational sophistication through the systematic mobilization of civilian expertise within a deeply militarized institutional framework. For NATO allies reconsidering force structure after Ukraine, the lesson is pointed – the most innovative military unit may be the one whose members hold the deepest civilian roots.

Keywords: reserve forces, innovation, capital

IEVA BĒRZIŅA*

POLITICAL LITERACY TO COUNTER HYBRID THREATS: LESSONS FROM LATVIA

*National Defence Academy of Latvia

Amid a transition from a rules-based world order to power politics, protecting physical and cognitive borders is a priority task for European countries to safeguard their sovereignty, territorial integrity, and fundamental democratic values. The article conceptualises 'political literacy' as a countermeasure to hybrid threats, which targets the political dimension among others. The paper distinguishes four essential aspects of political literacy for society's ability to resist hybrid threats: understanding of citizens' duty to defend the country; knowledge of the national and international security context; cognitive security; civic and political participation and examines how Latvian civic education prepares young people for them.

Keywords: hybrid threats, political literacy, civic education, Latvia

MORTEN BRAENDER*

WALK THE TALK? THE ANTECEDENTS OF DEFENCE-WILLINGNESS IN DENMARK

*Aarhus University

In Denmark, there has been very little interest in and very few studies focusing on territorial defence over the past 30 years. Now, for obvious reasons, the political discourse has changed radically. So has defence spending and public support for these. However, the begging question is whether the willingness to defend is also in place? This study aims to close this gap by using a representative sample (n=1000) of Danish citizens, asking whether the respondents are ready to defend their country and how they envisage that they can contribute concretely to this. Specifically, the study will centre on the antecedents of the defence-willingness: What explains the differences between those who will walk the talk and those who would prefer not to?

Keywords: defence-willingness, Denmark, public opinion

CARLOS MICHEL CALLIRGOS*

TRANS-INSTITUTIONALISATION AND THE DESIGN OF POST-SERVICE IDENTITY INFRASTRUCTURE: IMPLICATIONS FOR MILITARY FORCE SUSTAINABILITY

*Total Veteran Ltd.

Operational experience shapes military institutions from the inside. When infrastructure designed to receive those leaving fails to match the institutional character of what they carry out, the costs fall on force sustainability. This paper argues that translating operational insight into defence innovation must include the design of post-service infrastructure.

Drawing on Interpretive Phenomenological Analysis of veteran entrepreneurs and developing the Total Veteran model, the paper advances trans-institutionalisation: the process through which institutionalised identities, norms, and practices are carried across the military-civilian boundary and reconstituted within structurally compatible post-service forms. Military service produces durable institutional imprinting: values, behavioural orientations, and identity commitments persisting beyond formal exit. Yet transition infrastructure largely treats post-service challenges as navigational problems: employment, housing, and signposting. Where the institutional character of what veterans carry is unrecognised, institutional absence generates disorientation and adverse outcomes. Where structurally compatible forms exist, veterans rebuild coherence and contribute to civilian society and the broader defence community.

Three arguments follow. First, post-service identity continuity is a force-sustainability question: nations failing to provide adequate institutional infrastructure for veteran reinvention damage the social contract underpinning voluntary service and recruitment. Across NATO-aligned forces facing documented recruitment shortfalls, this is an operational concern. Second, effective post-service infrastructure must span three levels: micro (individual identity continuity), meso (peer-regulated reinventive community), and macro (symbolic and policy environment legitimating veteran identity in civilian life). Third, structural compatibility, the degree to which post-service forms echo the institutional character of military service, predicts which support designs will sustain adaptation, providing a testable basis for defence innovation.

The paper connects the Total Veteran model to the UK Strategic Defence Review 2025, NATO recruitment decline, and evidence (Sharp & Stevelink et al. 2025; Burdett 2024) that difficulties cluster most acutely among those whose exit is abrupt. Submitted to Armed Forces and Society.

Keywords: trans-institutionalisation, military transition, veteran identity, post-service infrastructure, force sustainability

STEFANO DE ROSA*

MILITARY SERVICE AND SOCIAL INTEGRATION: PEOPLE OF FOREIGN ORIGIN IN THE SWISS ARMED FORCES

*Military Academy at ETH Zurich,

Armed forces are commonly seen as one of the main symbols of a state. As an institution, they represent the unity of a nation. However, societies are often very diverse, and many are shaped by decades of migration. So, the question arises: how do the armed forces address the possibility of people from different origins serving in the military? Also, we must ask whether serving in the military may present an opportunity for people coming from abroad to integrate more into society. This presentation uses Switzerland as an example to answer these questions.

Using data from the Swiss Armed Forces (SAF), we discuss the potential opportunities and challenges of migrants serving in the military. How is their perspective on military service? Are their expectations and experiences different from those of people originally from Switzerland? What benefits may arise for the SAF and Swiss society?

We find various interesting dynamics associated with the military service of people of foreign origin. Differences occur in their expectations regarding the benefits of their service, in their motivation for military training, in their career intentions, and in their perception of camaraderie.

The results also suggest that there may be a general pattern in which minorities in a society serve in the military. Theoretical reflections – especially the theory of ethnic boundary-making – may help in understanding the findings. Finally, general recommendations are provided to better reconcile military service with the experiences of people of foreign origin.

Keywords: social integration, military service, foreign origin

GITANA DUDZEVIČIŪTĖ*

THE RESILIENCE OF SMALL STATE SOCIETIES IN THE CONTEXT OF PERCEPTIONS OF SECURITY

*General Jonas Žemaitis Military Academy of Lithuania

The resilience of societies in small states is becoming an increasingly important analytical framework for understanding how such states respond to a dynamic security environment and changing patterns of threat perception. Empirical studies show that the populations of small states are often more sensitive to geopolitical changes, making their perception of security highly dynamic and rapidly evolving. The aim of this research is to identify the factors shaping the resilience of Lithuanian and Estonian societies in the context of security perceptions, based on data from representative surveys conducted in 2022 and 2025. Automatic Linear Modeling (ALM) was applied in the analysis. The research results revealed that although Estonian residents continue to report higher levels of subjective safety, the proportion of individuals in Lithuania who feel safe increased from 45% in 2022 to 60% in 2025, whereas in Estonia it declined from 74% to 65% over the same period. At the same time, the resilience of Lithuanian residents increased, while that of Estonian residents decreased. Lithuanian society's resilience was most strengthened by preparedness for potential threats: having a prepared departure (survival) bag in case of evacuation, a willingness to defend the country in any possible way, and the perception of NATO membership as the most important factor ensuring the country's security.

Estonian society's resilience was most influenced by anxiety over a potential conflict between Russia and NATO, the perception of NATO membership as the most important factor ensuring the country's security, and the government's ability to adequately inform the public about potential threats and security measures. In summary, resilience and the perception of security in Lithuanian and Estonian societies are closely interrelated processes that shape small states' ability to remain stable, respond effectively to threats, and maintain social cohesion.

Keywords: resilience, security, societies, small states

OKSANA HUSS*

ROLE OF LOCAL SELF-GOVERNMENTS IN BUILDING LAYERED RESILIENCE: LEARNING FROM UKRAINE

*NATO Defense College and University Duisburg-Essen

Resilience has become a widely used but increasingly diffuse concept in responses to mounting crises and escalating wars, particularly where the boundaries between military and civilian responsibilities are blurred. While NATO's layered resilience concept helps structure resilience across military, civil, and societal dimensions, its broad application risks overlooking a governance gap, especially at the local level, where expectations for action often lack operational, political, and economic clarity. Drawing on Ukraine's experience of Russian full-scale war as a critical reference point, this analysis shows how local governance becomes decisive under extreme pressure; the paper introduces ten functions that local authorities can fulfil to strengthen layered resilience.

Keywords: layered resilience, Ukraine, local authorities

VYTAUTAS ISODA*

THE INVESTMENT IN AND TRANSFORMATION OF PARAMILITARY ORGANIZATIONS IN THE BALTIC STATES SINCE THE RUSSIAN INVASION OF UKRAINE

*General Jonas Žemaitis Military Academy of Lithuania

The existing academic literature on state-sponsored paramilitary and gendarmerie-type organizations mostly focuses on their role in civil wars, intra-state unrest, and counterterrorism. In the Baltic States, however, voluntary paramilitary organizations like the Lithuanian Riflemen's Union (*LŠS*) and the Estonian Defence League/Women's Home Defence (*Kaitseliit/Naiskodukaitse*) apart from being involved in community service are increasingly entrusted with armed territorial defence against a potential foreign enemy by their respective governments. This is not a typical model compared to other European countries that have paramilitaries of some kind and deserves an explanation as to why the governments of such small states like the Baltics allocate a significant part of their limited defence budgets to the paramilitary when their regular militaries are in need of procurement. This paper entails a comparative research design based on interviews with Lithuanian and Estonian policy-makers (both at the political and the bureaucratic levels) and document analysis. The aim is to describe the changes in the official tasks of such organizations and the trends in resources they possess over the last decade since the annexation of Crimea and particularly since the full-scale Russian invasion of Ukraine in 2022, as well as to explain the strategic, operational and tactical logic behind these changes. This paper is an attempt to move beyond the well-established field of civil–military relations (DCAF) in political science to explore (and possibly bring to the mainstream) the research on civil-paramilitary and military-paramilitary relations.

Keywords: paramilitary, Baltic States, defence policy

AUSRA KAMINSKAITE*

MEASURES TO RETAIN MILITARY PERSONNEL IN THE ARMED FORCES UNDER THE CURRENT SECURITY CONTEXT

*General Jonas Žemaitis Military Academy of Lithuania

Recent changes in the European security environment have raised new concerns. Like throughout all of Europe, the Lithuanian Armed Forces face challenges in attracting and retaining professional military personnel. The problem of recruiting and retaining quality people seems to be more or less universal. Even though the current security situation has increased societal attention and support towards strengthening the military and its personnel, the changing values of civil society, the increasing employment competition between the private market and the military, and a low unemployment rate combine to result in continued problems in military personnel retention. This conference paper is based on quantitative data analysis obtained through a survey. Data was gathered in 2026. This presentation focuses on a research question concerning the identification of effective, military service-based measures helping to retain soldiers in the military. Korsakiene, Lobanova, and Stankeviciene's (2019) theoretical model of the internal and external employee motivations was adopted and expanded for military personnel. The research results, based on the opinions of professional soldiers, identified problem areas and ways to improve them.

Keywords: retention, motivation, military personnel, security issues

KAIRI KASEARU*
ELERI LILLEMÄE[2], LIINA-MAI TOODING[3]

SOCIAL COHESION, MEDIA USAGE, AND PERCEPTION OF HYBRID THREATS WITHIN THE WHOLE-OF-SOCIETY APPROACH

*,[3]University of Tartu, [2]Estonian Military Academy

The whole-of-society approach to defence is founded on the principle of social cohesion, which includes sub-dimensions such as the willingness to defend, institutional trust, and patriotism. This approach provides a strong foundation for national defence, underscoring the importance of engaging the entire society and securing its support. However, it also encounters significant challenges, particularly from the risks of information manipulation and other hybrid threats that can weaken social cohesion.

This presentation aims to explore the relationships between social cohesion and the perception of hybrid threats within the context of the whole-of-society approach. The main question being addressed is how different information disorders, perceived as hybrid threats, relate to institutional trust and whether they influence the general willingness to defend. For this analysis, we utilize Estonian public opinion data collected from 2022 to 2025 (N=5000).

The primary research question is to identify the predictors of individuals' perceptions of threats. Hybrid threat perception is measured by three components: the spread of fake news, cyberattacks against various institutions, and hybrid attacks aimed at influencing Estonian politics or economics for personal gain. The main predictors in this study include media use, social media usage, social cohesion, expectations regarding the future security situation, and the perceived intensity of Estonian media coverage of the war.

Initial results indicate that individuals who believe the media covers too many war-related topics tend to have a lower perception of hybrid threats. At the same time, those who find the coverage appropriate generally perceive higher levels of hybrid threats. Furthermore, threat perception is more pronounced among the Estonian-speaking population and among those with higher levels of education. Additionally, social cohesion plays a significant role: the greater the sense of cohesion, the higher the perception of threat.

Keywords: hybrid threats, social cohesion, media, societal resilience

MARO KETOLA*
TEIJA SEDERHOLM[2]

FINNISH VOLUNTARY NATIONAL DEFENCE AS A PILLAR OF TOTAL DEFENCE

*-[2]Finnish National Defence University

This study examines how volunteers are able to support public authorities during disruptions or emergency conditions, thereby contributing to the whole Finnish total defence system. The Finnish defence system includes total defence, which is a combination of all the national and international military and civilian measures to enable homeland defence in all security situations. The cornerstones of Finnish defence are an evolving conscription system, a large, well-trained reserve, and a strong will to defend the country. When considering potential future crises and emergency conditions, it is important to understand and recognise the key role that trained volunteers play in safeguarding societal resilience and ensuring total defence.

Finns' interest in voluntary national defence has increased significantly since the outbreak of the war in Ukraine. There is a desire to learn new and to strengthen existing skills. They ask what I could do in a crisis situation. The role of citizens and organizations is a central part of Finland's comprehensive security model.

For this study, interviews were conducted with 14 public authorities and voluntary organizations involved in total defence. The study aims to identify new tasks, the need to develop training and skills, and current gaps in the involvement of volunteers in defence-related tasks now and in the future. The data clearly shows that there is a demand for more active participation of volunteers among the authorities. Voluntary organizations themselves have also worked actively to make their contributions more visible and to make the authorities aware of the organizations' expertise and capabilities. This study contributes to a broader discussion on a whole-of-society approach, defence capabilities, and gives insights into how to improve volunteer integration into the Finnish total defence system.

Keywords: voluntary national defence, societal resilience, non-governmental organisations, total defence

ROBERTS KITS*

CITIZEN ENGAGEMENT IN COUNTERING HYBRID THREATS: READINESS TO REPORT SUSPICIOUS ACTIVITIES IN THE BALTIC STATES

*University of Latvia

In recent years, Europe has faced a sharp increase in hybrid threats, including acts of sabotage and attacks on critical infrastructure, as well as espionage, disinformation campaigns, cyberattacks, and other forms of malign interference. As the threat landscape grows more complex, public authorities actively involve citizens in the monitoring and reporting of suspicious activities. This development signals a changing relationship between the state and society, in which citizens are no longer conceived as passive recipients of security or merely expected to be self-sufficient in times of crisis, but instead as active contributors to national resilience.

Given their exposure to regional tensions, the Baltic states need to foster resilience across the whole of society. Drawing on a 2026 public opinion survey conducted by the University of Latvia in the three Baltic capitals – Tallinn, Riga, and Vilnius – the data show that, despite efforts to promote a comprehensive defence system in which responsibility for defence and resilience is shared between the state and individuals, many respondents still perceive it primarily as the state's task. At the same time, individual freedoms are valued more highly than public security. Although people in the Baltic region express a general willingness to report suspicious activities and acknowledge the importance of individual involvement in public security and resilience, notable gaps remain – particularly regarding how to report, whom to report to, and whether reporting meaningfully contributes to overall public security.

This presentation will outline the main findings and awareness gaps identified in the public opinion surveys, with particular attention to statistically significant differences across demographic groups in the three Baltic capitals. It will also present insights from ongoing research on how modern technologies can be used to close existing gaps in citizen involvement in countering hybrid threats.

Keywords: suspicious activities, hybrid threats, Baltic states, resilience

KRISTINA KIVISTIK*
KAIRI KASEARU[2]

SECURITIZATION IN ESTONIAN POLITICAL DISCOURSE: NON-CITIZENS' VOTING RIGHTS IN THE CONTEXT OF LOCAL GOVERNMENT COUNCIL ELECTIONS

*-[2]University of Tartu

Russia's full-scale invasion of Ukraine has demonstrated how war can transform understandings of citizenship, political participation, and security within democratic societies. One of the processes accompanying such geopolitical shifts is securitization**.** This paper examines the securitization of non-citizens' voting rights in local government council elections in Estonia during the constitutional amendment process in the Riigikogu. Drawing on the Copenhagen School's securitization theory, and employing Lene Hansen's poststructuralist discourse analysis, the study analyzes parliamentary debates surrounding the amendment of the Constitution of the Republic of Estonia (536 SE). The empirical material consists of transcripts from the three readings of the constitutional amendment bill. The findings demonstrate that non-citizens' voting rights were predominantly framed as a security issue rather than solely as a matter of democratic participation. Securitizing discourses emphasized sovereignty, foreign influence, and loyalty, constructing non-citizens' voting rights as a (potential) security threat, whereas desecuritizing discourses highlighted the lack of evidence for such threats, social cohesion, and the rule of law. The analysis further reveals substantial differences among political actors in their understanding and application of security arguments. While political actors broadly acknowledged the changed security environment following Russia's full-scale invasion of Ukraine, they differed considerably in how they interpreted its implications for non-citizens' voting rights. Some actors supported the constitutional amendment on security grounds, others advocated stricter restrictions, while some questioned the necessity and proportionality of the proposed measures. The legislative process also reflected discursive change, as securitizing discourses became increasingly consolidated over time. Taken together, these findings illustrate how shifting security environments may reshape understandings of political participation in democratic societies.

Keywords: securitization, citizenship, political participation

MARCEL KOLB*

CIVIL-MILITARY COOPERATION FOR MARITIME CRITICAL INFRASTRUCTURE PROTECTION: FROM AD HOC LIAISON TO INTEGRATED DEFENCE PREPAREDNESS

*Johns Hopkins SAIS and NEXMARIS GmbH

This paper examines how civil-military cooperation can be made operationally useful for protecting maritime critical infrastructure, especially offshore wind farms, subsea cables, ports, maritime logistics, and energy corridors. It does not treat “whole-of-society resilience” as a broad policy slogan, but focuses on the concrete interface between armed forces, civilian ministries, infrastructure operators, regulators, coast guards, police, municipalities, and private contractors.

Recent incidents in the Baltic and North Sea have shown that maritime security is no longer a purely military task. Critical infrastructure at sea is often privately owned, civilian-operated, internationally connected, and legally complex, yet it may become the target of sabotage, espionage, coercion, or grey-zone disruption. This creates a practical civil-military cooperation problem: armed forces may hold surveillance, planning, and response capabilities, while civilian actors often control the infrastructure, technical knowledge, maintenance capacity, and first indicators of abnormal activity.

The paper asks how civil-military cooperation can be structured so that operational insights from infrastructure operators and security authorities are translated into actionable defence preparedness. It analyses the gap between formal crisis-management frameworks and the practical requirements of early warning, information sharing, joint exercises, escalation, and response coordination.

The central argument is that the main innovation need is institutional rather than purely technological. Better sensors and surveillance systems are necessary, but insufficient if actors lack trusted contact points, shared reporting formats, pre-agreed escalation thresholds, and regular exercises before a crisis occurs.

The paper contributes a civil-military cooperation model for maritime infrastructure protection built around five functions: shared situational awareness; permanent liaison structures between armed forces, coast guards, regulators, and private operators; escalation protocols; scenario-based exercises; and continuity planning that links military protection with civilian redundancy, emergency repair, public communication, and economic resilience.

Keywords: Baltic sea, civil-military cooperation, hybrid threats, infrastructure

DAVID LAST*

SURVIVING THE GREY ZONE: NATIONAL IDENTITY, COHESION, AND PROTECTING INSTITUTIONS

*Royal Military College of Canada

Must armed forces change to defend society? Grey zone threats include cognitive warfare, lawfare, infiltration, contracted attacks, cyber-attacks, and economic warfare. Infiltration of public institutions, elite capture, and covert influence or intimidation of diaspora communities distort policy from within. Adversaries contract attacks through organised crime, sabotage critical infrastructure, and disrupt with cyber-attacks. Economic pressure, supply-chain manipulation, targeted sanctions, and concealed strategic investment can degrade livelihoods, widen social fractures, and delegitimise government. The connections that make states prosperous can make them vulnerable. The identity of multicultural democracies is at stake. Openness creates vulnerability. When partners turn predatory, institutions can become vectors of threat. Language, communication channels, collaborations, shared information, and the habits of generations cannot be quickly changed. A framework for approaching resilience describes how foundational resources, providers of essential goods and services, and enabling capacities interact to determine resilience in the face of disruptive pressures. Society needs material foundations, effective governance, social cohesion, and timely and accurate policy responses to withstand shocks. How can multicultural states protect the institutions that preserve their identity? Examples of threats, policies, laws, regulations, and practices are drawn from a multinational comparison and applied to Canada. The result is a matrix of vulnerabilities and the tools available to the democratic state to protect its institutions. The matrix suggests some innovative uses for armed force, which may require a revised social contract with violent professionals.

Keywords: resilience, infiltration, cognition, legitimacy, vulnerability

JÚLIA LOPES*

FROM LIBERAL PEACEBUILDING TO SOCIETAL RESILIENCE? (RE)INTERPRETING THE WOMEN, PEACE, AND SECURITY AGENDA IN CONTEMPORARY DEFENCE GOVERNANCE

*Brazilian Army Command and General Staff College (ECEME) and Danish Institute for International Studies

Contemporary security environments are increasingly shaped by prolonged conflicts, hybrid threats, humanitarian crises, and growing demands for adaptation. Within this context, the Women, Peace, and Security (WPS) agenda faces new challenges regarding its strategic relevance and institutional role in contemporary security governance. Originally institutionalized within liberal peacebuilding and post-conflict frameworks, the WPS agenda is increasingly intersecting with broader debates on military adaptation, civil preparedness, and whole-of-society approaches to security. This paper investigates how the agenda is being (re)interpreted in response to these evolving challenges and within ongoing processes of military adaptation and societal resilience, using Denmark as a case study.

Drawing on literature on defence governance, resilience studies, strategic culture, and National Action Plans, this paper analyses how changing security dynamics influence the institutional role of WPS within Danish defence and security policy. The study also incorporates emerging discussions on women's civil society participation in contemporary conflict settings. Through qualitative document analysis of Danish National Action Plans, strategic policy documents, and recent policy debates, the paper examines how WPS principles are being integrated into broader frameworks of security governance and institutional adaptation.

The paper argues that contemporary insecurity does not necessarily marginalize the WPS agenda, rather, it contributes to its strategic reinterpretation as part of wider processes of societal resilience, civil preparedness, and defence transformation. By bridging WPS and gender studies with military sciences, the research contributes to current debates on the social dimensions of contemporary security governance.

Keywords: women, peace and security agenda, national action plans, Denmark, institutional adaptation, governance

LY LUKS*
KAIRI KASEARU[2]

FEMALE CONSCRIPTS' DROP-OUT RISK AND INTENTION TO JOIN EDF AS AN ACTIVE-DUTY MEMBER

*-[2]University of Tartu

Changes in the security environment and the promotion of gender equality have led to greater inclusion of women in national defence. Previous research has shown that both individual motivational factors and service experience influence enlistment and retention in the armed forces, yet less is known about how these factors shape women's service trajectories in countries where female participation in conscript service is voluntary. The study examines predictors of voluntary dropout among female conscripts and explores the relationships among enlistment motivations, service experiences, and intentions to pursue a military career. It relies on data from the Estonian Defence Forces' human resources survey, focusing on women who enlisted between 2020 and 2024 (N=259).

The results showed that enlistment motivations did not predict voluntary dropout within 90 days, while educational level emerged as a more relevant factor. Intention to continue in active service was predicted by a duty and career measure from the beginning of service, and by the Defence Forces identity measured at the end of service. It also emerged that some women begin conscript service with already established attitudes toward active service. The findings suggest that preventing voluntary dropout requires greater attention to service experience and background factors than to enlistment motivations, and that the sense of belonging developed during service plays an important role in supporting the intention to continue in active service.

MARIA MURUMAA-MENGEL*
ANASTASIA ISABELLA POOLE[2], SIGRID AAS[3]
INFLUENCER-STRATEGIES USED IN SECURITY POLITICS AND WAR: ANALYSING SOCIAL MEDIA COMMUNICATION OF POLITICAL/MILITARY ELITE ACTORS

*[-2] University of Tartu, [3] University of Tartu and Estonian Military Academy

Consequently, social media introduces new forms of threat and reshapes how security is perceived (Nissen 2015). It also alters the conditions under which security scenarios are constructed and disseminated: platforms enable ordinary users, political/military elites, and influencers to communicate directly with followers (Barberá 2015), and these interactions can themselves evolve into security risks (Umansky 2022). Building on these dynamics, we examine how influencer practices creep into security politics during crises through a three-pillar framework - securitization, mediatization, and influencer creep.

Conceptually, we view securitization as strategic practice (Balzacq 2005; 2015), where audience, political agency, and context determine whether a mandate to act is granted. The mediatization pillar foregrounds how media logic and selective exposure structure security communication (Hjarvard 2008; van Dijck & Poell 2013). The influencer creep pillar explains how visibility tactics, such as personal branding, optimization, and authenticity, migrate into adjacent fields, including politics and security (Mears 2013). Extending this, we incorporate recent work on war influencers on TikTok (Burgess 2021; Divon & Krutrök 2025).

Empirically, our presentation draws on the currently ongoing study – semi-structured interviews (n=15) conducted with Estonian top politicians and defense services professionals. Elite political and military actors occupy privileged positions within securitization processes due to their institutional authority, symbolic capital, and access to public visibility. Traditionally, military communication has been embedded within collective institutional structures that limit individual expression. Social media challenges this model by enabling individual leaders to communicate directly under their own names, often through personal accounts. We demonstrate that platform logics and influencer practices recalibrate the balance between elite authority and networked publicity in times of crisis, making securitization a visibly negotiated, audience-dependent process.

Keywords: influencers, security, mediatization, social media

NEERAJ*

WHOLE-OF-SOCIETY DEFENCE IN A MULTIPOLAR ERA OF PERSISTENT HYBRID CONFLICTS: INDIA'S CIVIL-MILITARY INTEGRATION AS A MODEL FOR EU STRATEGIC AUTONOMY AND RESILIENCE

*Panjab University

In today's multipolar world, wars do not end quickly. As of May 2026, conflicts like the Russia-Ukraine war (now in its fourth year), Sudan's civil war, and unrest in Myanmar continue with no clear end. These fights combine traditional battles with new methods such as cyberattacks, drones, disinformation, and damage to roads, power plants, and other infrastructure. They affect not just soldiers but entire societies.

This paper examines how armed forces and society can work together more closely to become stronger. It focuses on India's whole-of-nation model as a helpful example for Europe. In India, defence is not only the military's responsibility. It brings together civilians, veterans, industries, and communities to handle disasters, border security, and new skills training. India keeps strong civilian leadership over the military while dealing with many threats and a diverse population.

The EU-India Security and Defence Partnership, signed in January 2026, offers a good opportunity to share these ideas. The partnership covers sea security, cyber threats, counterterrorism, and joint defence production. Europe is facing its own problems: difficulty in recruiting young people, lower public trust in the military, and hybrid pressures from other countries. India's experience in building public support and social unity can help Europe improve its own defence readiness and independence.

The paper presents a simple 'Multipolar Resilience Framework' with four main parts: protecting society from false information, making better use of people (youth and veterans), using new technologies in a fair way, and running joint training with civilians and military. It shows that close civil-military ties are a powerful strength for lasting peace and deterrence in long conflicts.

By learning from each other through this partnership, India and the EU can create more united societies ready for future challenges. This paper offers practical suggestions for joint exercises, research, and meetings to make the partnership truly effective and support wider global stability.

Keywords: whole-of-nation model, EU-India Security and Defence partnership, Multipolar Resilience Framework

KHALID SHAFI*
JENS MATHIESEN[2]

MILITARY SUPPORT TO CIVIL AUTHORITIES AND SOCIETAL RESILIENCE: PAKISTAN'S EXPERIENCE OF COVID-19 AND CLIMATE-RELATED EMERGENCIES

* NDU, Pakistan, Institute of Strategic Studies, Research and Analysis, [2]RDDC

The role of armed forces in contemporary security environments is no longer limited to conventional defence tasks. Pandemics, climate-induced disasters, public health emergencies, and humanitarian crises increasingly affect governance, social stability, and national resilience. This paper examines this evolving role through a focused case study of Pakistan.

The central research question is: How did Pakistan's armed forces support national crisis coordination and societal resilience during COVID-19 and subsequent climate-related emergencies, and what lessons does this experience offer for military sciences and defence planning? This paper treats Pakistan as the main case study, while using South Asia only as the wider regional and climatic context.

Methodologically, the study adopts a qualitative case-study approach, using process tracing across two crisis episodes. First, the COVID-19 response, with particular reference to the National Command and Operation Centre (NCOC); and second, military support during climate-related emergencies, especially floods and disaster-relief operations. The evidence base includes official policy documents, public statements, disaster-management material, available public health and climate-risk data, and relevant academic and policy literature.

The analysis is guided by a civil-military resilience framework built around three dimensions: coordination and governance, military support functions, and resilience outcomes. The first dimension examines how civil and military institutions coordinated during national crises. The second looks at military contributions such as planning, logistics, mobility, communications, field deployment, and inter-agency coordination. The third considers how these arrangements affected institutional coherence, continuity of governance, public communication, and emergency response capacity.

The paper argues that Pakistan's experience shows the value of armed forces as a force multiplier in complex domestic emergencies, particularly where civilian systems face capacity constraints. The paper concludes that future defence institutions will need stronger doctrine, training, and civil-military mechanisms for supporting national resilience in an era of compound security risks.

Keywords: armed forces and society, societal resilience, climate security, crisis governance

KRISTJAN SILM*
TIIA-TRIIN TRUUSA[2]

MAKING DEFENSE PERSONAL: NARRATIVE PATHWAYS INTO VOLUNTARY DEFENSE IN ESTONIA

*University of Tartu, [2]Baltic Defence College and University of Tartu

Russia's full-scale invasion of Ukraine has once again raised the question of citizens' 'will to defend'. Using Estonia as an example, we examine how people's abstract 'will to defend' becomes an active contribution to national defense through a voluntary defense organization. We analyze 25 narrative interviews with people who voluntarily joined the Estonian Defense League between 2022-2024. As a result, the article outlines four paths to joining: transforming fear into capability, war as a turning point, the feasibility of a life path, and changing the organization's image. The article shows that people do not simply join in response to threats; they translate attitudes, moral emotions, identity, and practical possibilities into concrete defense actions.

Keywords: will to defend, comprehensive national defense, voluntary defense participation, Estonian Defense League, threat perception, narrative interviews, moral identity

SILVIA SOMMARBERG*
VESA VALTONEN[2], TEIJA SEDERHOLM[3]

WATER SECURITY DURING CASCADING DISRUPTIONS: INSIGHTS FROM SCENARIO WORKSHOP IN FINLAND

*-[3]Finnish National Defence University

Access to safe water is a basic societal function, yet in situations of severe disruption or military threat, it can quickly change into a strategic vulnerability.

In Finland, water security is discussed through the framework of total defence and societal resilience. Finland's comprehensive security model brings together public authorities, infrastructure operators, volunteers, civil society, and defence organizations in preparedness and continuity planning. In addition, resilience and civil preparedness have become a growing focus within NATO. This is particularly embedded in Article 3 and NATO's seven baseline requirements for national resilience, which emphasize the continuity of government, continuity of essential services to the population, and civil support to military operations.

Building on scenario-workshop discussions, the study explores how different actors perceive strengths, vulnerabilities, and cooperation during different disruptions of normal conditions. In some scenarios, familiar risks and responsibilities were combined with sudden and unexpected developments. While many risks to water services are identifiable and manageable under normal conditions, their character may significantly change when society moves towards emergency conditions. Particular attention is given to dependencies between critical systems such as water, energy, and logistics, as well as how disruptions may cascade across society.

The study examines how water security actors, public authorities, volunteers, and other preparedness actors interpret their roles, mandates, and cooperation when routine arrangements are placed under strain. By approaching water infrastructure as a critical societal function, the discussion contributes to wider debate on societal resilience, civil preparedness, civil-military cooperation, and national defense in contemporary security environments.

This study is a part of SafeWaterForAll project funded by Research Council of Finland.

Keywords: water security, total defence, comprehensive security, societal resilience

RONEY SOUSA*

JOINT AND INTERAGENCY GOVERNANCE IN HYBRID SECURITY ENVIRONMENTS: OPERATIONAL INSIGHTS FROM THE CATRIMANI OPERATION

*Brazilian Army Command and General Staff School (ECEME)

This paper derives operational insights from the Brazilian Joint Operational Command Catrimani, treated as a field laboratory for joint and interagency cooperation against cross-border environmental crimes in the Amazon. Drawing on my experience as J5 (Plans), I examine how military and civilian actors coordinated efforts to disrupt illegal mining and related illicit flows in the Yanomami Indigenous Territory under a demanding legal, political, and humanitarian context.

Using the Institutional Collective Action framework, the paper analyses how governance arrangements and coordination mechanisms supported cooperation among the three armed services and multiple federal agencies. It focuses on the design of command-and-control structures, planning routines, and information-sharing practices aimed at reducing friction and transaction costs in a multi-actor, multi-level environment.

The paper then connects these operational insights to ongoing debates on defence transformation in hybrid security settings. It shows how concrete experiences from Catrimani informed adjustments in joint command procedures, standard operating procedures, and interagency coordination protocols. The argument is that operations against environmental crimes in border regions, although below the threshold of conventional war, provide a valuable testbed for organisational innovation and doctrinal development in contemporary military sciences.

Keywords: joint and interagency operations, defence governance and transformation, hybrid security environments

STEPHEN TRYNOSKY*

CLOSING THE GAP: A NEW CONCEPTION FOR NATO RESERVE COMPONENTS IN AN ERA OF GREAT POWER COMPETITION

*US Army War College and The George Washington University

The Russia-Ukraine War has upended many post-Cold War strategic assumptions across the NATO alliance. Among the most significant lessons from the conflict is the enduring centrality of mass in large-scale military operations against peer and near-peer adversaries; specifically, personnel, equipment, and magazine depth. The heightened possibility of protracted, attritional warfare on NATO's Eastern Flank demands a long-overdue re-examination of the Alliance's strategic manpower depth in comparison with the Russian Federation which mobilized over 300,000 reserve personnel in late 2022 – its first mobilization since 1941. After more than four years of war, Moscow still maintains a reserve military mobilization pool of over 2,000,000 pretrained personnel available for recall. The growing gap between NATO and the Russian Federation's strategic personnel depth threatens the Alliance's ability to maintain credible deterrence and meet anticipated wartime operational requirements if deterrence fails.

This paper, initially commissioned by the NATO Defence College, examines the disparate "multiverse" of national approaches to reserve manpower across the NATO Alliance which range from robust "total defense" systems to chronically understrength all-volunteer militaries. It then uses quantitative and qualitative methods to comparatively explore the reserve systems that have sustained both Moscow and Kyiv's war efforts which were structured and employed very differently from the unit-centered, "operational reserve" model currently common among the largest NATO militaries. Finally, the study employs comparative scenario construction and evaluation methodology to identify and assess several actionable options for NATO member states to both grow their reserve manpower pools and accelerate wartime mobilization timelines. The paper argues that the present reserve force structure and mobilization assumptions for most NATO militaries are inadequate for high-intensity conventional war and will be further complicated by political, logistical, and social factors amidst the backdrop of crisis.

Keywords: reserve, manpower, strategic depth, mobilization, deterrence, protracted conflict

DÁNIEL BERNÁT VAY*

FUTURE OF THE MILITARY WORKFORCE IN NATO'S EASTERN FLANK: POLICY INNOVATION TO MITIGATE DEMOGRAPHIC CONSTRAINTS

*Corvinus University of Budapest and Hungarian Defence Forces

NATO's eastern flank states – Estonia, Latvia, Lithuania, Poland, Slovakia, Hungary, Romania, and Bulgaria – differ in their military development, capabilities, traditions, political systems, geographic features, security perceptions, demographic trends, social acceptance of military service, and economic resources. Yet they all confront a similar dilemma. As potential frontline states, they face greater and more direct military pressure due to their geopolitical position near the Russian Federation and Belarus.

The NATO Allies, in response to a rapidly changing security environment, are obliged to launch robust, comprehensive force development programs to meet increasing military requirements in both quantity and quality in order to maintain NATO's credible deterrence and defence posture. The European governments, with very few exceptions, took new directions in their approach to military security and placed their defence spending on an upward trajectory, but they still must address the fundamental paradox. The rising defence spending has not solved Europe's soldier shortage, as shrinking youth populations and low military attractiveness leave forces understaffed. The eastern flank is more strongly affected by demographic trends and, in addition, by emigration within the European Union, while benefiting less from migration flows on the continent.

The paper examines the current state capacity of eight eastern flank states, measured through a three-level funnel: the demographic ceiling, the legal and political ceiling, and actual extraction to project the possible pool of human resources for 2044. Additionally, it signals the challenges these states will face in military workforce planning as their populations continue to shrink and age.

Beyond diagnosis, the paper identifies concrete areas where policy innovation could increase human resource extraction within existing demographic constraints: expanding the eligible recruitment base through gender-inclusive service policies, optimising reserve and territorial force models, and reducing legal-political barriers between the demographic and actual extraction ceilings

Keywords: NATO, eastern flank, military workforce, policy innovation, demography

AULI VIIDALEPP*

SOCIOCULTURAL VULNERABILITIES EXPLOITED IN AI-ENABLED HYBRID INFLUENCE ACTIVITIES

*University of Tartu

AI-enabled disinformation is becoming commonplace and is considered a threat to democratic societies. AI-enhanced “propaganda factories” allow influence actors to deploy vast volumes of linguistically sophisticated and contextually adaptive messages that overwhelm discourse and mimic grassroots sentiment across platforms. Such operations destabilize the interpretive environment by creating uncertainty about the authenticity of information and the intentions, identity, and ideological affiliations of involved actors. The resulting cognitive overload can erode situational awareness, complicate threat assessments, and delay or distort operational and institutional decision-making.

Fears and expectations related to generative AI systems often stress the inevitability and the damaging technological potential of AI. Less attention is paid to the sociocultural factors that both underlie and enable the exploitative activities. This research argues that sociocultural factors are equally important to study. Historical contextualization of information operations and a semiotic study reveal the underlying cultural communication mechanisms and open new perspectives to address the problems.

Generative AI technologies, as accelerated fake production systems, enable the exploitation of existing semiotic vulnerabilities. Disinformation operations take advantage of three sociocultural issues: the (dis)trust in factual authority, the discourse of fear, and weak referentiality in generative AI output. Understanding these sociocultural processes is essential for increasing the resilience of societal, institutional, and deliberation practices.

Keywords: generative AI, information influence, cognitive warfare

DAĞHAN YET*

ASYMMETRY OF COMFORT

*Turkish National Defense University

Modern Western military interventions are increasingly defined by a profound structural vulnerability where an adversary's 'asymmetry of will' effectively paralyzes Western strategic execution. Building upon Andrew Mack's foundational concept of the asymmetry of will, this presentation introduces the 'Asymmetry of Comfort', arguing that the West's strategic failure in protracted conflicts is rooted in a societal 'glass jaw' created by an extreme aversion to risk and casualty. While traditional strategic analyses frequently emphasize the economic sustainability or material costs of prolonged conflicts, this paper posits that the primary constraint on modern military decision-making is fundamentally political. Specifically, it is the electoral survival of policymakers, driven by an acute societal intolerance to casualties in the face of highly motivated opponents.

Utilizing a phenomenon-to-concept approach, this study traces the root of this strategic paralysis through a four-stage structural transformation of European war rationality. First, it examines the profound ontological shift in the state-citizen relationship. The sanctification of the individual has repositioned the modern state as a specialized service provider, systematically eroding the traditional historical rationale for collective sacrifice. Second, drawing on Azar Gat's perspectives regarding the pacification of daily life, the paper highlights how the complete exile of physical violence from the Western public sphere has reduced societal tolerance for physical risk to absolute zero. Third, it analyzes the resulting instrumentalization of military service. Modern armed recruitment is increasingly driven by financial rationality rather than existential civic devotion.

Finally, these factors culminate in the structural collapse of the Clausewitzian Trinity during contemporary 'wars of choice'. Absent an existential threat to the homeland, combat casualties cease to be acceptable military friction; they instantly transform into severe domestic political crises that directly threaten electoral survival, forcing Western decision-makers into a permanent state of strategic paralysis.

Keywords: war studies, military sociology

WORKING GROUP 8:
DEFENCE MANAGEMENT AND ECONOMICS

Chair

MARKUS GAUSTER
Austrian National Defence Academy

Co-Chair

CHRISTOPHER JOHN YOUNG
Baltic Defence College

IMOH ANTAI*

PRE-LOGISTICS DUE DILIGENCE IN DEFENCE AND MILITARY GROWTH: ABSORB, BLEND, OR COMBINE?

*Swedish Defence University

In an era marked by geopolitical competition, disrupted supply chains, rapid technological advancements, and mounting demands for military preparedness, defense organizations are under increasing pressure to expand their capabilities while preserving operational resilience. This growth can occur organically, through force expansion, infrastructure development, and capability modernization, or inorganically, through acquisitions, strategic partnerships, alliance integration, and defense-industrial consolidation. Despite the importance of logistics to military effectiveness, logistics considerations are often addressed only after growth decisions have been made, which increases the risk of capability gaps, inefficiencies, and strategic vulnerabilities.

This paper introduces the concept of Pre-Logistics Due Diligence (P-LDD), a strategic framework that assesses logistics readiness before organizational growth initiatives are undertaken. Based on fieldwork within the Swedish Armed Forces, the paper expands the traditional due diligence concept in management literature by evaluating supply chain factors, such as sustainment capacity, logistics resilience, integration, supplier dependency, transportation networks, maintenance capabilities, digital platforms, and transformation processes, as factors that can enable sustainable military growth. The framework proposes that successful defense growth depends not merely on acquiring or developing new capabilities or platforms but also on understanding how those capabilities can be integrated into a logistics growth infrastructure. To guide decision-making, this paper presents an integration typology with three strategic pathways: Absorb, where new capabilities are incorporated into existing logistics structures; Blend, where legacy and new systems coexist through selective integration; and Combine, where a new logistics architecture is deliberately created from both existing and emerging capabilities. The study positions logistics as a strategic enabler rather than a supporting function by linking logistics theory to military readiness, supply-chain resilience, and organizational growth. The proposed framework provides military planners, policymakers, and defense leaders with a new way to evaluate growth decisions in an increasingly uncertain global security environment.

Keywords: logistics due diligence, growth, organic, inorganic, supply chain

FATMA CENGİZ*

EARLY WARNING FOR DISRUPTION RISK IN DEFENCE PROCUREMENT: FROM REACTIVE REGISTERS TO ANTICIPATORY SIGNALS

*Independent Researcher

Delay and disruption are chronic problems in defence procurement. Cost overruns, slipping schedules, supplier failures, and sudden geopolitical shifts repeatedly delay the delivery of capabilities that armed forces are counting on. The way programmes are usually managed, however, stays one step behind. Risk registers and milestone reviews record what has gone wrong at fixed checkpoints, and established tools such as earned-value tracking read mainly from past performance, yet they say little about the disruption that is still building beneath the surface.

This paper sets out an early-warning approach for detecting that build-up before it turns critical. Instead of assessing risk as a snapshot, the model reads observable programme and environmental indicators (schedule drift, cost-growth momentum, single-source dependency, sanction exposure, decision latency) and turns them into ongoing warning signals. The aim is to catch emerging trouble while intervention is still cheap and still possible. It is meant as a decision-support tool, not a prediction machine: it does not claim to forecast outcomes, only to point managers toward the conditions where a programme is most likely to stall.

The approach is grounded in a comparative study of national procurement systems across several countries, together with a set of programme case studies, from stalled efforts such as the UK Ajax to rapidly delivered and widely exported systems such as South Korea’s K9 Thunder, that show how these indicators behave before trouble surfaces. Two things follow. The first is conceptual: a case for moving procurement risk management away from logging failures after the fact and toward anticipating them. The second is practical: a sketch of how mixed, uneven indicators can be combined into early-warning scores that managers can actually read and act on.

Treating procurement disruption as something to detect early rather than account for later aligns with the conference’s interest in turning operational experience into usable innovation. It offers defence managers a concrete instrument grounded in real programme histories rather than another after-action lesson.

Keywords: defence procurement, early warning, disruption risk, decision support, anticipatory risk management

ANTONIO JOÃO DE OLIVEIRA VIANNA JUNIOR*
GABRIELA ROCHA BERNARDES[2]

STRATEGIC CAPABILITIES OF THE DEFENSE INDUSTRIAL BASE: A COMPARATIVE STUDY BETWEEN BRAZIL AND NATO COUNTRIES

*-[2]Brazilian Army Command and General Staff School (ECEME)

This presentation aims to analyze and compare the strategic capabilities of Brazil's Defense Industrial Base (DIB) in relation to the member countries of the North Atlantic Treaty Organization (NATO). The research adopts a qualitative approach, operationalized through a comparative case study as its central methodological strategy, enabling the identification of similarities, divergences, and gaps in the development of defense industrial capabilities between Brazil and the key Western actors within the collective defense framework. The study is classified as exploratory, descriptive, and comparative, combining a systematic literature review of the specialized literature in defense economics, document analysis of institutional reports – such as those published by the Brazilian Ministry of Defense, the European Defence Agency (EDA), and NATO – and the analysis of selected industrial capability indicators (defense R&D expenditure, share of GDP, defense exports, and degree of technological autonomy). The time frame covers the year 2025, encompassing Brazil's current standing and the post-2014 modernization and interoperability efforts of NATO member states. The study examines key dimensions, including technological autonomy, R&D intensity, indigenous production capacity of critical systems, and integration into global defense supply chains. The analysis seeks to understand how Brazil, despite remaining outside NATO's collective defense architecture, positions its DIB in terms of strategic capabilities to confront shared challenges – such as national sovereignty, technological dependency, and industrial competitiveness. Beyond the bilateral comparison, the article offers reflections on lessons the Brazilian experience can provide to NATO countries for developing a DIB under resource-constrained conditions, and vice versa, contributing to the academic debate on models of defense industrial policy in both emerging and developed economies.

Keywords: defense industrial base, strategic capabilities; NATO; Brazil

ANTONIO JOÃO DE OLIVEIRA VIANNA JUNIOR*
KARINA FURTADO RODRIGUES[2]

A COMPARATIVE ANALYSIS OF DEFENSE INDUSTRIAL BASE INCENTIVE POLICIES: BRAZIL X LEADING EU NATIONS

*-[2]Brazilian Army Command and General Staff School (ECEME)

This study conducts a structured comparative analysis of public policies designed to foster the Defense Industrial Base (DIB) in Brazil, Spain, Germany, and France. By focusing on these four specific nations, the research seeks to identify convergences, divergences, and the structural determinants that shape their respective policy trajectories. The research employs the method of structured, focused comparison, examining the cases across three interconnected analytical layers: structural, geostrategic, and policy specific.

The structural layer assesses innovation rankings, state capacity, and industrialization/deindustrialization trends, investigating how these factors condition each actor's ability to develop and sustain a robust DIB. The geostrategic layer examines alignment with major powers versus strategic autonomy, participation in economic and military blocs, and the existence of declared adversaries. This highlights the fundamental asymmetry between the three European nations – operating within NATO's collective defense architecture and the EU framework – and Brazil's autonomous positioning outside formal military alliances.

The policy layer focuses specifically on DIB incentive instruments. It compares Brazilian mechanisms, such as the Special Tax Regime for the Defense Industry (RETID) and the Special Procurement Term (TLE), with European and national-level instruments. This includes collective frameworks like the European Defence Fund (EDF) and Permanent Structured Cooperation (PESCO), as well as the specific industrial participation and national procurement policies of Spain, Germany, and France. The research is currently in the data collection and analysis phase, with results expected to shed light on how distinct institutional and geostrategic contexts shape defense industrial policy outcomes. The study aims to contribute to the academic debate on defense industrial policy models in both emerging and developed economies.

Keywords: defense industrial base, public policy, Brazil, Spain, Germany, France, comparative analysis

VLAD DUMITRACHE*

HOW DEFENSE ACQUISITION HAS EVOLVED IN A EUROPEAN CONTINENT WHERE RE-ARMING HAS BECOME A PRIORITY

*National Defense University 'Carol I'

Ever since the European Union chose to launch the Rearm Europe Initiative and develop the SAFE Instrument, European countries have tried to juggle between using their own national defense resources and using lending instruments that have become available at EU level. These alternatives, however, raise concerns as economic pressure could impact long-term national commitments for many of those willing to access funds for defense purposes. The aim of this paper is to analyze how the countries on the Eastern Flank have strategized and adopted a balanced path for attracting specific funds for defense acquisition. Case studies will be drawn from the separate approaches of Poland and Romania. What makes this path a difficult one, what are the impediments to accessing loans, and how is the decision-making process for defense acquisition influenced by other variables, such as the strategic partnership with the United States of America become questions worth pursuing during the several chapters of this scientific work.

Keywords: defense acquisition, resources management, national GDP, reimbursement mechanisms

HELIO CAETANO FARIAS*

IN SEARCH OF STRATEGIC AUTONOMY: EUROPEAN DEFENCE INDUSTRIAL FINANCING MECHANISMS AND LESSONS FOR BRAZIL

*Brazilian Army Command and General-Staff College (ECEME)

The intensification of geopolitical competition, the war in Ukraine, and the fragmentation of global supply chains have placed the defence industrial base back at the center of national and regional security strategies. Since 2016, and at an accelerated pace following 2022, the European Union and its member states have strengthened political consensus around the need to reinforce the European defence industrial base, reduce strategic dependencies, and expand defence production capacity. These developments reflect a broader shift in which defence policy has become increasingly intertwined with industrial policy, technological innovation, and geopolitical competition.

This paper examines the main mechanisms mobilized by the European Union to strengthen its defence industrial base, with particular emphasis on the European Defence Fund (EDF) and the European Defence Industry Programme (EDIP). It investigates how these instruments seek to transform growing defence expenditure into sustainable industrial capabilities by addressing procurement fragmentation, production bottlenecks, and vulnerabilities in critical supply chains. Attention is given to the role of financing arrangements, coordinated procurement, industrial mobilization, and incentives for technological development in expanding Europe's defence production capacity and strengthening strategic autonomy. The research adopts a qualitative approach based on the analysis of official documents, budgetary data, and public policy reports. Drawing on the literature on Defence Economics, Geopolitics, and Defence Industrial Policy, the study assesses the relationship between threat perceptions, industrial mobilization, and state-led coordination mechanisms.

The central argument is that recent European initiatives represent an effort to align defence planning, industrial capabilities, and long-term strategic objectives through new financing arrangements and industrial policy instruments. Beyond the European case, the paper explores the implications of these developments for Brazil. It argues that the European experience provides lessons for the design of financing instruments, long-term procurement policies, and industrial coordination mechanisms capable of strengthening Brazil's Defence Industrial Base.

Keywords: defence industrial base, geopolitical competition, strategic autonomy, EU, Brazil

JOÃO XAVIER GONÇALVES*

FROM OPERATIONAL LESSONS TO FUNDED CAPABILITY: DEFENCE BUDGET ADMINISTRATION, RESOURCE ALLOCATION AND STRATEGIC READINESS IN PORTUGAL

*Academia Militar

This paper examines how defence budget administration shapes a small NATO ally's ability to translate operational lessons, strategic priorities, and burden-sharing commitments into funded, deployable, and innovative military capabilities. Using Portugal as an illustrative case, it asks: how does the composition of defence expenditure affect the translation of operational insight into credible capability development and strategic readiness?

The study adopts a qualitative exploratory-descriptive methodology, combining documentary and bibliographic analysis with a structured reading of NATO and Portuguese defence expenditure indicators. The analysis focuses on the balance among personnel, operations and maintenance, equipment investment and modernisation, and relates these categories to NATO benchmarks, capability-based planning, and Portuguese strategic defence documents. This approach allows the paper to assess not only how much is spent, but what expenditure enables in terms of readiness, interoperability, innovation, and deployability.

The central argument is that defence budgeting should be understood as a strategic translation mechanism: it converts political ambition and operational experience into force structure, readiness, procurement priorities and military innovation. Contemporary conflicts have reinforced the importance of stockpiles, sustainment, air defence, cyber resilience, unmanned systems, logistics, interoperability, and industrial responsiveness. In this context, aggregate expenditure is insufficient as a measure of defence effort if the budget is heavily absorbed by personnel and routine operations, thereby limiting investment in equipment, training, maintenance, and emerging capabilities.

The paper contributes to the ISMS 2026 theme by proposing a three-level analytical framework that links strategic ambition, budget composition, and capability output. Applied to Portugal, the framework highlights the tension between fiscal discipline, NATO commitments and military modernisation, while offering a defence management perspective on how operational insights can be converted into sustainable, interoperable and innovation-oriented military power.

Keywords: defence management; defence budgeting; resource allocation; capability development; Portugal; NATO; strategic readiness

GUSTAV GRANLUND*

ACCELERATING DEFENCE INNOVATION IN SWEDEN: INSTITUTIONAL BARRIERS AND PATHWAYS FOR CIVIL-MILITARY-INDUSTRY COORDINATION

*Swedish Defence University

This thesis defines the structural characteristics of an optimally functioning Swedish defence innovation system and identifies the institutional barriers that prevent the current architecture from reaching that optimum. Russia's full-scale invasion of Ukraine in 2022 has triggered the most comprehensive Swedish rearmament since the 1950s, yet capability demand cannot be met by scaling existing production alone; contemporary defense requires integrating disruptive technologies at iteration tempos for which Sweden's peacetime institutions were not designed.

A composite Optimisation Framework is constructed by integrating Horowitz and Pindyck's three-stage innovation process model (invention, incubation, implementation), Terhorst's moderating conditions, the Triple Helix model of civil-military-industry coordination, the DOTMLPFI capability taxonomy, and a statutory-artefact category specific to the Swedish administrative tradition. The framework is refined for SMEs and startups through a Founder Origin distinction. Wartime Ukraine serves as an empirical comparative reference, not a prescriptive model.

Applied diagnostically to the Swedish institutional record, the framework surfaces nine structural gaps distributed across the three stages together with three cross-stage feedback failures, concentrated in incentive design, SME and startup entry asymmetry, procurement, and security classification filters (LOU and the Protective Security Act), prime-contractor channel capture, and institutional contact-avoidance (*beröringsskräck*). Each gap is attached to the institutional principal positioned to act on it, and recommendations are organised around three architectures: information and feedback, actor configuration and entry, and procedural and risk allocation.

Keywords: defence innovation, civil-military-industry coordination, triple helix, DOTMLPFI, institutional barriers

JAROSŁAW GRYZ*

ENERGY CHAINS IN NATO'S MULTI-DOMAIN OPERATIONS

*War Studies University

The high energy demand of machines, devices, vehicles, and platforms poses a serious challenge to provide them with this during the preparation and conduct of multi-domain operations. The lower energy density of alternative fuels compared to fossil fuels requires a fundamental redesign of future machinery, equipment, vehicles, and platforms. The energy demand of the military in multidomain operations will exceed the capacity of traditional energy sources to sustain forces in the future operational environment, regardless of scale. This will require significant investment from the military, and the current fossil fuel distribution infrastructure cannot be upgraded to support zero-emission platforms (both electric and hydrogen) and will have to be built from scratch. The level of technological readiness of non-missionary technologies and their performance in extreme operational conditions is not yet suitable for machines, equipment, vehicles, or military platforms. It should be emphasized that if this transformation is not carried out in an appropriate way, there will be a significant reduction in the capabilities of the armed forces in confrontation with an adversary using new methods of obtaining, distributing, and using energy. Fossil fuel supply chains will be even more vulnerable in the environment of large-scale combat operations. New types of energy supply chains will need to be resilient, efficient, and interoperable, and to provide access to energy in the challenging environment of the armed forces. This problem applies to all types of troops and domains (land, sea, air, space, cyber). The aim of the chapter is to examine the nature of changes in non-hydrocarbon forms of energy in energy supply chains in order to meet the growing energy needs of machinery, equipment, vehicles, and platforms, while requiring a transition to more resilient energy supply systems in multi-domain operations, with particular emphasis on the impact of the energy transition.

Keywords: energy, NATO, MDO

ROLAND HELLBERG*
DAVID MANNING[2]

LOGISTICAL SUPPORT REQUIREMENTS OF THE DISPERSED AIR BASE SYSTEM

*Swedish Defence University, [2]Freelance Lecturer and Writer, Senior Enlisted Member of US Air Force

The renewed emphasis on dispersed air operations following Russia's full-scale invasion of Ukraine has made the US-led Agile Combat Employment (ACE) concept central to NATO air power planning. While ACE has received considerable attention as an operational concept for enhancing survivability through dispersion, its underlying logistics model remains comparatively underdeveloped. This paper critically evaluates the logistics assumptions underpinning ACE by examining whether current approaches provide sufficient resilience to sustain high-tempo air operations in contested environments. Drawing on historical Swedish air base concepts, NATO doctrine, and contemporary developments in military logistics, the study compares three alternative approaches to dispersed air operations: the traditional centralized collocated operating base model, the ACE concept, and the Swedish Bas 90-inspired system.

The analysis argues that the effectiveness of dispersed air operations depends less on aircraft dispersal itself than on the resilience, integration, and adaptability of the supporting logistics system. Four interrelated logistical challenges are identified: (1) sustaining distributed stocks of aviation fuel, munitions, spare parts, and other critical supplies across dispersed and austere operating locations; (2) coordinating logistics, maintenance, and operational command to enable rapid aircraft turnaround; (3) ensuring mobile support capabilities and decentralized decision-making through highly trained personnel; and (4) maintaining resilient supply chains when transport infrastructure, communications, and host-nation support are disrupted or contested.

The paper argues that the current ACE concept places greater emphasis on operational manoeuvre than on the organizational and logistical architecture required to sustain operations. As an alternative, the Swedish model illustrates how dispersed air operations can be supported through integrated logistics organizations, pre-planned infrastructure, pre-positioned resources, and strong civil-military coordination. The study concludes that future NATO air power would benefit from complementing ACE with a more comprehensive logistics support model capable of sustaining prolonged dispersed operations under contested conditions.

Keywords: dispersed air basing; agile combat employment, air power sustainability; military airbase logistics

NICK WALTER HEINRICH HUSMANN*

CROSSING THE VALLEY OF DEATH: HOW RESOURCE ALLOCATION LOGICS SHAPE MILITARY INNOVATION SUCCESS UNDER CONDITIONS OF SCARCITY AND INSTITUTIONAL UNCERTAINTY

*Military Academy at ETH Zürich and the Swiss Armed Forces

The ability to convert emerging technologies into operational capability has become a central determinant of defence effectiveness, as highlighted by the war in Ukraine. Yet European defence institutions continue to struggle with the "Valley of Death": the transition phase where decision-makers allocate scarce resources based on noisy performance signals, and where non-linear cost escalation risks eliminating viable projects before they reach operational readiness. While existing research identifies institutional barriers, the interaction between allocation design and project survival remains underexplored. The central question is under which informational conditions uniform allocation outperforms selective allocation in sustaining viable projects through the Valley of Death.

An agent-based model (ABM) simulates a portfolio of projects as agents progressing through TRL 4 to 7, facing escalating capital requirements and declining advancement probabilities. A funding authority allocates a fixed budget either uniformly across projects or selectively to those with high observed performance signals subject to noise. The model formalises how signal distortion and behavioural constraints interact with allocation rules to generate premature attrition or sustained portfolio diversity.

Parameter ranges draw on expenditure benchmarks from the European Defence Agency (EDA) and the European Defence Fund (EDF). A plausibility check combines rule verification through extreme-value testing with pattern matching against known empirical regularities: elevated project attrition rates in the Valley of Death phase, and funding-threshold effects on advancement probability. PESCO attrition rates serve as reference only, given the distinct political determinants of collaborative project failure.

We expect the performance advantage of selective allocation to erode sharply once signal noise exceeds a critical threshold. Under uncertainty levels typical of European procurement environments, uniform allocation is expected to yield higher aggregate success rates by preventing early termination of viable projects. We further expect that allocation reform in fragmented institutional settings should prioritise noise-robust distribution mechanisms over merit-ranked concentration of resources.

Keywords: agent-based modelling, defence innovation, Valley of Death, resource allocation, military procurement, bounded rationality, European Defence Fund

JĀNIS KONDRĀTS*
JELENA PUNDURE[2], INGA JEKABSONE[3], ASTRA AUZIŅA-EMSIŅA[4], MARTINS VARGULIS[5]

FROM DEFENCE INNOVATION TO ECONOMIC VALUE: AN EMPIRICAL ASSESSMENT METHOD FOR SMALL-STATE ECONOMIES

* - [4]Riga Technical University, [5]PowerHouse Latvia

Defence innovation is increasingly framed as a source of military capability, technological sovereignty, and economic value. Existing empirical studies examine defence R&D, military expenditure, defence-industrial performance, and defence-to-civilian spillovers, but they rarely measure the economic contribution of defence innovation ecosystems as a distinct object of analysis. This gap matters for small states, where the defence sector is narrow, demand is strongly shaped by public procurement, and not all defence-related production can be treated as innovation. This paper asks: how can we measure the economic value created by defence innovation ecosystems in small states? The article develops an empirical assessment method and applies it to Latvia as a small-state case. The method first defines the boundary between the wider defence industry and defence innovation by identifying firms, research organisations, and public actors involved in the development of new or improved defence and dual-use technologies. It then measures economic contribution through a focused set of observable indicators: innovation-related turnover, employment, R&D activity, public support, procurement links, exports, and dual-use commercialisation. The study does not claim to estimate a full macroeconomic multiplier. Instead, it offers a transparent and replicable way to assess the measurable economic contribution of defence innovation ecosystems using available firm-level, public-sector, and statistical data. The article contributes to defence economics by moving from sector mapping towards a more precise measurement of how defence innovation creates economic value in small-state economies.

Keywords: defence innovation, innovation ecosystem, defence industry policy, economics

LINUS KÜHL*

AN INDICATOR-BASED FRAMEWORK FOR ASSESSING HYBRID VULNERABILITIES IN ALLIED LOGISTICS SUPPLY CHAINS

*FH Münster University of Applied Sciences

Security of supply has returned to the centre of allied defence planning, yet the tools planners can actually reach for remain split into two silos: static quantitative models built on historical economic and transport data, and subjective, slow-to-update expert country judgements. Neither gives an operational audience a timely, standardized basis for deciding where to harden first. The gap is sharpest where modern threats concentrate, in hybrid vulnerabilities, where a sanctioned flag-state denial, a cyber-frozen port, a sabotaged corridor, or a sole-source dependency compound one another faster than any single discipline tracks.

This proposal addresses that gap with a deliberately accessible instrument: an indicator-based framework that captures hybrid vulnerabilities and single points of failure across allied supply chains and condenses them into a decision-ready picture. The doctorate began in October 2025 and is at the design stage; what follows is the proposed method. First, indicator design: a parsimonious set of indicators spanning geographic and chokepoint concentration, sole-source and single-corridor dependency, transport-mode substitutability, flag-state and carrier exposure, sanctions and export-control exposure, and cyber-layer fragility, each with a transparent definition, data source, and scoring rule. Second, single-point-of-failure detection through dependency mappings between supplier and transit states. Third, aggregation, with explicit weighting and sensitivity checks, into a compact vulnerability profile per commodity and corridor that ranks where hardening yields the most resilience per unit of effort. Fourth, illustration and planned validation against the 2021-2024 crisis episodes (Suez, Red Sea, Russia-Ukraine corridors, Panama Canal drought); no empirical results are claimed at this stage.

The contribution is a transparent, reproducible, low-barrier method that bridges quantitative country-risk research and indicator-driven reporting practice into a tool operational planners can adopt. Primary fit: WG8 (Defence Management and Economics), with cross-cutting relevance to WG3 and WG6.

Keywords: security of supply; hybrid threats; supply-chain resilience; logistics country risk; single point of failure; indicator framework; NATO logistics; defence economics

RINGAILĖ KUOKŠTYTĖ*

CAPACITY, NETWORK CAPITAL, OR CONVERGENCE? CENTRAL AND EASTERN EUROPEAN COUNTRIES IN THE EUROPEAN DEFENCE FUND (2022–2024)

*General Jonas Žemaitis Military Academy of Lithuania

Central and Eastern European (CEE) countries face a structural tension in the European Defence Fund (EDF), the EU's main instrument for co-financing collaborative defence research and capability development: the programme offers access to European defence-industrial networks while its competitive architecture may systematically favour established Western incumbents. Using EU Financial Transparency System (FTS) data for 2022–2024, this study examines whether EDF allocation patterns among CEE member states are more consistent with defence-industrial capacity, network capital, or financial convergence dynamics. Defence-industrial capacity is associated with EDF allocations, consistent with a supply-side explanation. Yet many CEE countries appear underpredicted by this relationship. Additionally, the paper examines whether consortium leadership as a form of network capital helps account for variation within the CEE group. This finding reveals a bifurcated CEE landscape in which coordinator access, rather than accession cohort, separates active leaders – notably Estonia, Latvia, and Slovenia – from marginal participants. Finally, some evidence of financial convergence is found – countries starting from lower allocation bases tend to grow faster, suggesting that structural position is not permanent.

Keywords: Central and Eastern European countries, European Defence Fund, defence-industrial capacity, consortium leadership, convergence

YAN KWIZERA*

THE ZIPLINE EFFECT: SOVEREIGN FRONTIER INFRASTRUCTURE AS A CATALYST FOR ACCELERATING MILITARY INNOVATION CYCLES

*HuzaX

The primary challenge facing contemporary Western military innovation is the “Sclerotic OODA Loop”, a systemic bottleneck where domestic regulatory friction and prescriptive certification standards throttle the maturation of autonomous systems. While synthetic modeling offers a baseline for testing, the “Sim-to-Real” gap can only be bridged through high-volume operational “mileage” that is increasingly difficult to achieve within traditional Western testing ranges.

This paper introduces the Sovereign Frontier Infrastructure (SFI) framework as a strategic methodology to bypass these institutional barriers. Using the “Zipline Model” as a primary case study, we analyze how a performance-based regulatory environment facilitated over one million autonomous flight hours in a complex, real-world setting. This operational density enabled a rate of hardware iteration and sensor-fusion hardening unmatched by traditional defense procurement. The research argues that by utilizing allied emerging markets as high-velocity regulatory sandboxes, NATO and AUKUS-aligned forces can achieve “Mission Readiness” long before frontline deployment.

The adoption of SFI necessitates a rigorous ethical mandate to ensure the pursuit of technological overmatch does not compromise the agency of host populations. We propose a “Shared-Value Governance” model, where the integration of autonomous systems provides immediate, measurable civilian benefits – such as emergency logistics or infrastructure support – that offset the risks of field experimentation. To manage these challenges, this framework mandates three core safeguards: (1) *Proportionality*, limiting testing to dual-use technologies where civilian utility is the primary driver; (2) *Transparency*, requiring local sovereign authorities to maintain full visibility into performance metrics; and (3) *Civic-First Verification*, ensuring systems meet baseline civilian safety thresholds before iterative defense-related testing occurs.

By grounding SFI in these pillars, the Venture Operating model transforms into a symbiotic partnership. We conclude that SFI is a critical geopolitical tool for maintaining technological overmatch, provided that innovation remains subordinated to the sustainable development and explicit consent of the host sovereign nation.

Keywords: sovereign frontier infrastructure, venture operating, defense procurement, regulatory sandboxes, autonomous systems

TIAGO MARQUES DOS SANTOS FILHO*

OVERCOMING TECHNOLOGICAL DEPENDENCY IN SMALL UNMANNED AERIAL SYSTEMS (UAS): A TRIPLE HELIX MODEL FOR DUAL-USE MICRODRONES IN THE BRAZILIAN ARMY

*Brazilian Army

Modern tactical environments increasingly rely on Category 0 and 1 Unmanned Aerial Systems (UAS/Drones) for reconnaissance, surveillance, and target acquisition. However, the Brazilian Army faces a critical strategic vulnerability due to its high technological dependency on foreign off-the-shelf microdrones. This dependency creates severe logistical and operational constraints, threatening strategic autonomy and information security. The study will utilize the Triple Helix Model as its core conceptual framework to analyze how institutional spheres – the Military/Government, Academia, and the Defense Industry – can foster an integrated innovation ecosystem. By framing the development under a dual-use perspective, the research explores how civilian technological capabilities and military operational requirements can converge to generate scalable, sovereign solutions. The research adopts a qualitative and exploratory research design centered on the Brazilian defense innovation ecosystem. The empirical data consists of structured interviews with key stakeholders across the Triple Helix, including military decision-makers, defense industry executives, and academic researchers. Additionally, a comparative analysis of institutional frameworks and operational requirements is conducted to identify bottlenecks in national technology development. Preliminary results indicate that overcoming the dependency on foreign microdrones requires a structured shift from generic defense procurement to collaborative, codesigned R&D programs. By leveraging the Triple Helix dynamics, the Brazilian Army can position itself as a key anchor customer and innovation partner, aligning military operational status tracking with civilian manufacturing capabilities. The study provides a strategic roadmap for local mass production of dual-use UAS components, enhancing national defense autonomy while stimulating the domestic high-tech industrial base.

Keywords: Triple Helix model, unmanned aerial systems, tactical drones, defense industry, dual-use technology, Brazilian Army

MASHUDU MATHOHO*

ASSESSING RENEWABLE ENERGY READINESS ON MILITARY BASES: A GEOSPATIAL ANALYSIS OF SOLAR ENERGY ADOPTION IN THE WEST COAST REGION OF SOUTH AFRICA

*Stellenbosch University

Energy resilience is no longer a civilian luxury but a strategic military necessity considering grid instability, rising energy costs, and an evolving geopolitical landscape. This study assesses the readiness of selected South African National Defence Force installations in the West Coast region to transition towards solar photovoltaic energy as a pathway to enhanced operational sustainability and energy security. A geospatial multi-criteria decision analysis integrating Geographic Information Systems and the Analytic Hierarchy Process was applied to evaluate four bases: Saldanha Military Area, Air Force Base Langebaanweg, 4 Special Forces Regiment, and Air Force Base Ysterplaat, using environmental, infrastructural, and operational criteria, including solar irradiance, land surface temperature, slope, aspect, land cover, and proximity to transport networks. The weighted overlay model identified Saldanha and Langebaanweg as highly suitable due to favourable terrain and solar potential, while spatial and urban constraints reduced suitability at the remaining installations. Beyond site selection, the study demonstrates how geospatial decision-support tools can strengthen defence energy planning, reduce vulnerability to external supply disruptions, and contribute to climate-responsive military infrastructure. The findings advance the discourse on renewable energy as a force multiplier in the defence sector and support evidence-based pathways towards low-carbon, energy-secure military systems.

Keywords: energy security, GIS-MCDA, solar energy, defence sustainability, renewable energy planning

PETER PAPLER*

INNOVATION-DRIVEN DEFENSE ORGANIZATIONS

*New University Faculty of Government and European Studies

The Russo-Ukrainian War, the US-Iran war with proxy-backed campaigns in the Middle East, and the Israel-Hamas conflict have accelerated a fundamental reassessment of defense organization, force design, and military innovation across western armed forces. These wars have demonstrated that traditional hierarchical structures and lengthy capability development cycles are increasingly inadequate in operational environments characterized by rapid technological adaptation, pervasive sensing, autonomous systems, and continuous battlefield experimentation. Contemporary military organizations are therefore shifting toward innovation-centric models that integrate operational feedback, technological development, and capability generation into a single adaptive ecosystem. The approach is the establishment of Capability Directorates functioning as institutional innovation hubs responsible for identifying operational problems, coordinating experimentation, and accelerating the transition of novel technologies into military service. Such organizations increasingly resemble venture capital ecosystems rather than traditional procurement bureaucracies. At the tactical level, military units are adopting principles such as rapid prototyping, iterative testing, user-centered design, and continuous adaptation. Combat formations are becoming active contributors to capability development rather than passive recipients of centrally managed solutions. This trend has led to the creation of Concept Development Centres that operate as military start-ups, where the military, engineers, industry partners, and academic institutions collaborate to develop and validate new concepts under realistic operational conditions. Furthermore, recent conflicts have highlighted the vulnerability of large, permanent military installations to precision-strike systems. Consequently, armed forces with distributed force structures based on deployable capabilities, temporary operating locations, and training-area-centric models are examined. In these concepts, armed forces maintain minimal permanent infrastructure while relying on dispersed training facilities, pre-positioned equipment, digital command networks, and rapidly deployable formations. The resulting transformation represents a shift from industrial-age military institutions toward innovation-driven defense organizations capable of generating operational advantage through continuous adaptation, accelerated learning, and decentralized capability development.

Keywords: innovation, defense organization, force structure, unit as start-up

ASHU PASRICHA*

THE ECONOMICS OF PEACE IN EUROPE: A GAME-THEORETIC FRAMEWORK FOR CONFLICT PREVENTION AND DEFENCE INNOVATION

*Panjab University

The Russian invasion of Ukraine has exposed a structural gap in European security economics: deterrence spending, defence innovation, and procurement coordination are analysed in separate literatures, yet they constitute a single strategic coordination problem. This paper proposes the first integrated game-theoretic framework that simultaneously models deterrence investment, alliance innovation diffusion, and procurement coordination as three interconnected games linked through Bayesian updating 1. Operationalised against SIPRI and NATO data, the framework identifies a critical attribution reliability threshold below which hybrid provocations go unpunished in equilibrium – explaining why Russia's proxy and cyber operations systematically exploit attribution ambiguity – and quantifies the premium-to-payout ratio of deterrence investment at approximately 1:4, each euro spent on deterrence avoiding four euros in expected conflict costs. Comparative analysis of Poland, Germany, the Baltic States, and France reveals that Europe is trapped in a fragmentation equilibrium characterised by 178 weapon systems against 30 in the United States and a collaborative procurement rate of 18% against a 35% target. The paper introduces an Indian equilibrium comparison – asymmetric, doctrine-driven deterrence achieving comparable credibility at roughly 50% lower GDP share – and derives testable conditions under which each equilibrium dominates. Findings suggest that closing the attribution gap through collective intelligence, establishing a European Defence Industry Authority to reduce procurement fragmentation, and differentiating innovation obligations by member type can shift the equilibrium toward sustainable peace. The central argument is that peace in post-Ukraine Europe is not the absence of war, but a dynamic equilibrium sustained by deliberate investment in deterrence credibility, innovation capability, and institutional adaptation.

Keywords: game theory, defence economics, peace economics, deterrence, defence innovation, NATO, burden-sharing, hybrid warfare, European security, India, conflict prevention

GALINA ŠEVČENKO-KOZLOVSKA*

FISCAL AND ECONOMIC RISKS OF RAPIDLY GROWING DEFENCE EXPENDITURE: A STUDY OF PUBLIC FINANCE SYSTEM TRANSFORMATION

*General Jonas Žemaitis Military Academy of Lithuania

Since 2022, European defence expenditure has shifted from a cyclical to a structural fiscal commitment, driven by NATO's new 5% of GDP target and a deteriorating security environment. While the EU's national escape clause and the SAFE instrument provide temporary fiscal flexibility, defence spending remains one of the most rigid components of public expenditure, raising concerns about debt sustainability, crowding out of productive public spending, and the long-term resilience of public finance systems – particularly in small, high-exposure economies. This study examines the fiscal and economic risks associated with rapidly growing defence expenditure, using Lithuania – where defence spending reached a record 5.38% of GDP in 2026 – as a primary case, benchmarked against Latvia, Estonia, and selected higher-debt NATO members. The analysis applies internationally recognised methodologies. Publicly available data from SIPRI, Eurostat, the IMF, the European Commission, and national fiscal authorities underpin the empirical work. The paper contributes policy-relevant recommendations for managing fiscal risk during sustained defence-driven public finance transformation.

Keywords: defence expenditure, fiscal risk, public debt sustainability, public finance transformation

SALMA SHAHEEN*

THE RISE OF INFORMALITY IN EDT GOVERNANCE: PRIVATE SECTOR DYNAMICS AND NUCLEAR-ARMED STATES

*King's College London

Scholars have argued that states' growing vulnerabilities and the pressure to secure first-mover advantages in technological competition shape force modernisation around emerging and disruptive technologies (EDTs). These dynamics, in turn, hinder efforts to cooperate on the regulation and governance of such technologies. As a result, informality – understood as the lack of formalised institutional governance and the absence of international norms – has increasingly come to characterise this domain. Existing scholarship on EDTs has primarily focused on great power competition, deterrence and strategic stability, and arms-control challenges, while paying comparatively less attention to the role of the private sector in shaping the informal governance of national security. Consequently, a gap remains in international security scholarship regarding how this growing informality, alongside the rapid development of EDTs, affects national security. To address this question, this research comparatively analyses the role of the private sector in deepening such informality. Unlike traditional state-owned defence industries, the private sector operates through flexible innovation cycles, transnational investment networks, public-private partnerships, and dual-use technological development. This flexibility enables rapid innovation with limited regulatory oversight, often beyond the remit of existing arms-control and governance frameworks.

The study focuses on four nuclear-armed states – China, India, Pakistan, and the United Kingdom – and examines how the private sector has emerged as a key actor that states increasingly rely on for the development of novel national security capabilities. The findings suggest that increasing dependence on the private sector accelerates EDT development and intensifies strategic competition, further complicating efforts to establish formal international regulation and governance frameworks. The study argues that growing reliance on private-sector innovation is reshaping the relationship between technological competition and international security governance, contributing to fragmented regulatory architectures and weakening prospects for multilateral arms-control cooperation.

Keywords: emerging technologies, arms control, international security, military technology

MARIO JOSE SIMOES MARQUES*

BRIDGING OPERATIONAL INSIGHT AND DEFENCE INNOVATION: EU AND NATO RESEARCH PRIORITIES, SCIENTIFIC GAPS, AND OPPORTUNITIES IN CONTEMPORARY MILITARY TECHNOLOGY

*CINAV Escola Naval-Instituto Universitario Militar

The contemporary strategic environment in Europe is defined by a rapid transition from theoretical threat assessments to the analysis of live operational data, primarily driven by lessons from the high-intensity conflict in Ukraine. Institutional responses, notably the European Defence Fund (EDF) 2026 Work Programme and NATO's DIANA, have prioritised "Capability Maturation" (TRL 5–6) to bridge the persistent "Valley of Death" between laboratory research and operational deployment. However, significant sociotechnical and economic gaps remain that threaten the strategic credibility of European defence.

Cross-referencing institutional priorities with peer-reviewed literature reveals critical research voids. In air and missile defence, a 10:1 defensive cost-expenditure ratio renders the interception of hypersonic threats operationally unsustainable at scale. Autonomous systems and AI suffer from a lack of integrated security frameworks and a significant lag in Human-Machine Teaming (HMT) doctrine. Furthermore, operational-level AI remains structurally understudied, while NATO communications face an immediate "harvest-now, decrypt-later" quantum threat. Finally, hybrid warfare remains plagued by an "attribution-action gap" due to fragmented legal and operational frameworks.

To address these gaps, this paper proposes a prescriptive research agenda focused on actionable innovation. This includes prioritising *asymmetric counter-cost solutions*, such as low-cost autonomous interceptor swarms and directed energy, to reverse economic vulnerabilities in missile defence. It advocates for military education institutions to lead *standardised HMT red-teaming* in realistic environments to mitigate automation bias. Additionally, the immediate implementation of *hybrid cryptographic architectures* and the development of *"evergreen" procurement frameworks* are essential to overcome temporal asymmetries between evolving threats and solution timelines. These findings contribute to the ISMS 2026 theme by translating operational insights into credible, scalable defence capabilities

Keywords: research gaps, military technology, funding opportunities, European defence, actionable innovation

LENA TRABUCCO*
ALEXANDER HØGSBERG TETZLAFF[2]

THE TRANSFERABILITY OF UKRAINIAN INNOVATION: A FOUR-LAYER FRAMEWORK FOR SMALL STATES

*-[2]University of Copenhagen

How can states, especially small states, adopt lessons learned in Ukrainian military innovation without being under the hostile and tested conditions of an armed conflict? This paper answers this through a four-layer innovation framework – hardware, software and data, tactics and doctrine, and organisation and procurement – to disaggregate Ukrainian wartime innovation and assess what small states can realistically adopt. Denmark serves as our test case – a country undergoing budget expansion, force-structure reform, and a changing threat landscape.

We examine each layer for its characteristic innovation dynamics, from distributed UAV and naval-drone manufacturing to decision-support and targeting software, to small-unit experimentation and decision-making compression, to the procurement reforms and feedback structures. However, this scale and pace of innovation depend on certain enabling conditions, such as existential stakes, mass battlefield feedback, a deep technical talent pool, regulatory permissiveness, and civil-military integration. These enabling conditions are not currently transferable for Danish defense. We identify areas of innovation that may be immediately actionable in the current European landscape, while disaggregating other innovation practices which may not be immediately applicable.

Overall, this paper examines layers of innovation as an operational insight rather than as a self-evident driver of transformation. Each layer of innovation must be filtered through domestic institutional and strategic contexts before it can become actionable innovation. The four-layer framework, while applied in a Danish context, is applicable to other small states in the region.

Keywords: military innovation, military technology, Ukraine

LOUISE TUMCHEWICS*

SECURING THE UAV SUPPLY CHAIN

*University of Southern Denmark and Royal Danish Defence College

The war in Ukraine, as well as the conflict between Iran, the United States, and Israel, has demonstrated the utility of unmanned aerial systems (UAS) in contemporary combat. To de-risk from security dependence on the United States and foster European defence innovation, European states are investing heavily in UAS systems, typically developed by small to medium enterprises in an open innovation process. However, on close examination, these commercially available off-the-shelf systems (COTS) are reliant on component parts almost exclusively machined and manufactured in China. Indeed, a 2025 survey of UAS supply chains indicates that over 90% of components are manufactured in China.

To study this phenomenon, this paper analyses supply chains for UAS, using Svensson's supply chain analysis framework. It applies Farrell and Newman's concept of weaponised interdependence and expands it to transnational supply chains entwined with defence, politics, diplomacy, and national security. Whilst scholars and policy makers have expressed concern over rare earth elements and semi-conductors, this paper focuses on an understudied problem for small and medium states: the deep dependence on China for component parts, such as power supply units, motors, propellers, in commercially available systems, as well as the consequences for defence innovation and technological sovereignty. This paper demonstrates that this dependence was not inevitable, but the outcome of long-term defence and economic policies. This paper maps supply chain vulnerabilities, identifies critical chokepoints, and explores how awareness of this dependency shapes a new logic in defence innovation and technological sovereignty. It concludes by offering a series of recommendations for Nordic and Baltic states to de-risk the UAS supply chain.

Keywords: drones, security policy, defence investment

KRZYSZTOF WIATER*
ADAM DUDA[2], MICHAŁ MARCINIAK[3]

FROM CONTRACTING TO CAPABILITY: A STATUTORY ARCHITECTURE FOR "ARMAMENT AGENCY 2.0" AND THE REFORM OF DEFENCE ACQUISITION IN A SURGE-SPENDING ERA

*-[2]NGL/SGH/PIDU, [3]Armament Agency/SGH

Poland is executing a defence modernisation programme of unprecedented scale, with expenditure exceeding 4% of GDP and multi-decade contracts for advanced air, air-defence, long-range fires, and digital capabilities. This surge exposes the limits of an acquisition system shaped during the "peace dividend" era of low spending dynamics and few major programmes. The present model concentrates on the contracting stage while dispersing planning, requirements definition, and sustainment across separate institutions, producing fragmented accountability. Critically, much of its operating logic rests on internal administrative acts rather than statute, undermining the predictability that long-horizon programmes and industry require.

This paper presents a reform blueprint – "Armament Agency 2.0" – developed within an expert team convened under the Polish Dual-Use Chamber. We argue that organisational change alone is insufficient and propose a coherent three-tier statutory architecture: a Defence Potential Act defining the instruments of capability-building beyond procurement; a dedicated Defence and Security Procurement Code calibrating ordinary, accelerated, and emergency procedures to operational conditions; and an Armament Agency Act establishing an executive agency with a full life-cycle mandate and stable, term-based governance.

Analytically, the contribution is a shift from a contract-centred model to capability management, integrating life-cycle cost, intellectual property and technical data rights, financing structures, and local content within a single accountable institution. The argument is grounded in comparative institutional analysis of mature agencies (DGA, DAPA, FMV, SSB) and a diagnosis of the Polish case, drawing on defence economics and the dynamic-capabilities perspective.

By translating operational lessons from the current threat environment into durable institutional innovation, the paper speaks to the conference theme and to small and medium states pursuing technological autonomy. It offers both a governance template and a concrete legislative pathway for defence procurement reform.

Keywords: defence acquisition, executive agency, life-cycle cost, defence economics, capability management, defence procurement reform, Poland

WORKING GROUP 9: MILITARY EDUCATION

Chair

ANNE MARIE HAGEN
Norwegian Defence University College

Co-Chair:

ÜLLE SÄÄLIK
Estonian Military Academy

ISRAEL ALVES DE SOUZA JÚNIOR*

MILITARY SCIENCES, BRAZILIAN EDUCATIONAL PROGRAMS, AND POTENTIAL PRIMARY OBJECTS OF STUDY

*Brazilian Army Command and General Staff School (ECEME)

This investigation is exploratory research within the field of Military Sciences and its overarching educational scope. The topic is limited to a discussion of the ontological and epistemological aspects of Military Sciences as a way to guide the scientific research and the design of educational programs. To advance this investigation, two research questions were formulated: What constitutes military sciences? And how have Military Sciences evolved as a scientific discipline, shaping Brazilian educational programs? These questions indicate that the research was prompted by the need for a deeper understanding of the scope of Military Sciences as a field of academic, theoretical, and applied inquiry, as well as an attempt to define its object of study.

The primary objective of this research is, therefore, to try to understand Military Sciences based on the evolution of scientific thought. To this end, a specific survey of potential definitions for Military Sciences was conducted, tracing its trajectory as a field in expansion. The methodology employed is qualitative, using the literature review as the basic analytical framework.

Thus, this research presents a discussion on the nature of Military Sciences (from empirical to systematised knowledge), a philosophical-epistemological reflection on its trajectory as a field, and Brazilian educational perspectives. At the very end, some remarks show the relevance of Military Sciences as a contemporary educational field, regarding Security and Defense as potential primary objects of study.

Keywords: military sciences, security, defense, objects of study, Brazilian educational programs

DAVID ATKINSON*

THE SPACE TO THINK: JUDGEMENT CONDITIONING IN PROFESSIONAL MILITARY EDUCATION – DECISION-FORCING CASES FOR MISSION COMMAND UNDER COGNITIVE PRESSURE

*York St John University and UK Centre for Army Leadership

Professional Military Education (PME) develops mission command as a doctrinal practice, preparing leaders to exercise accountable judgement where interpretation is contested and decision time is compressed. Contemporary command combines contestable narratives and influence environments ("cognitive warfare") with AI-enabled decision support. While AI can enhance situational awareness, it can also shape options and narrow "thinking space" where mission command relies on trust, initiative, and judgement. In AI-accelerated environments, situational representations remain provisional even as operational consequences become binding – so responsibility remains located at the point of human commitment. PME therefore requires not only doctrinal understanding, but judgement conditioning before commitment under uncertainty – where actions carry operational, reputational, and legitimacy consequences.

This paper presents Hypothetical Decision-Forcing Cases (HDFCs) designed to expose learners to contested interpretation, second-order risk, and responsibility. The method uses an S2C2R cycle: consequences/risk exposure → plural sense-making → decision tension surfacing → commitment → consequences and risk re-exposure. It is not an optimisation loop. Instead, it is designed to preserve human judgement under conditions where AI-enabled systems may prematurely narrow perceived options; it is a training design intended to make assumptions visible, preserve decision authority, and support reflective learning.

The paper reports an HDFC delivered at a UK analyst and decision-maker conference using a law-enforcement task-force scenario with information contestation. A panel made the committed decisions across two rounds, while ten tables recorded "would-be" decisions under the same information. This enables analysis of decision variance and convergence/divergence, including differences between committed authority and distributed shadow decisions. The paper concludes with implications for doctrine and leader development: how judgement conditioning complements war-gaming and rehearsals, and how PME can better assess decision quality where uncertainty, legitimacy, responsibility, and commitment are inseparable.

Keywords: professional military education, mission command, judgement, decision-forcing cases, cognitive warfare, legitimacy

FILIP BANÁŠ*

TESTING WARGAME-BASED PREPARATION IN A LIVE MILITARY EXERCISE: EXPLORATORY EVIDENCE FROM A CONTROLLED FIELD EXPERIMENT

*Masaryk University

Capturing tactical-level military effectiveness remains a persistent methodological challenge. While some authors emphasize qualitative schemes or large datasets, the need to capture corresponding leadership skills together with the correct way of force deployment leaves these studies short of solving the issue. Moreover, while questionnaires and VR tools are frequently employed to evaluate the impact of various treatments on military effectiveness, comparatively few studies do so during live military exercises. Existing research, therefore, leaves a gap between highly controlled experimental environments and the operational settings in which military decision-making actually occurs. This gap is particularly relevant for field commanders, whose performance heavily depends on the ability to translate information, doctrine, and battlefield awareness into effective action under time pressure.

This study, therefore, investigates whether wargame-based preparation influences tactical-level military effectiveness during a subsequent field exercise. It employs a controlled field quasi-experiment involving approximately 40 soldiers and field commanders. Participants were assigned to treatment and control platoons; treatment platoon commanders then completed a preparatory wargaming session prior to the exercise. Independent instructors assessed participants in subsequent live exercises through Behavioural Observational Checklists. Rather than treating military effectiveness as a single outcome, the design decomposed performance into observable behaviours associated with preparation, assault, and withdrawal phases of the exercise scenario. The resulting data enabled both composite performance assessment and component-level analysis.

The findings suggest that wargame-based preparation may improve performance in the early stages of the operation, although the observed effect was inconsistent and tended to disappear in later phases. Although the small sample size precludes strong causal claims, the study demonstrates a feasible approach for evaluating wargaming under realistic military conditions and contributes to the broader discussion of military effectiveness. Overall, the article highlights both the opportunities and methodological limitations of conducting field experiments in military environments characterized by low sample sizes and logistical constraints.

Keywords: wargaming, military effectivity, field experiment, live exercise, tactical level

PARENTEAU DANIC*

THE APOLITICAL STANCE OF OFFICERS IN AN ERA OF POLITICAL POLARIZATION: THE CENTRALITY OF CRITICAL THINKING IN THE EDUCATION OF OFFICER-CADETS

*Collège Militaire Royal de Saint-Jean (CMR Saint-Jean)

The dominant model of Western civil-military relations, famously conceptualized by Samuel Huntington in *The Soldier and the State* (1957), is predicated on the duty of "apoliticism" for officers. Central to maintaining civilian democratic control over the military is the requirement that officers remain politically neutral and refrain from partisan action. The rise in *political polarization* we are witnessing throughout the West, which appears to be affecting all sectors of society, risks undermining this fundamental principle. As noted by Schedler (2023), polarization divides national politics into "opposing imagined communities", where dialogue, debate, and consensus-building, which are at the heart of any democratic system, become more difficult to generate and sustain. Political polarization undermines the very duty of "apolitism" for officers (Urben 2026). Indeed, in a polarized society it is increasingly difficult to remain politically neutral, in other words, to keep one's distance from all partisan politics, as the whole of society seems to be caught up in a dynamic where everything becomes a power struggle structured around fundamental and irreconcilable differences.

This paper aims to reflect on how to provide officer-cadets with the intellectual tools they need to resist the knock-on effects of political polarization, in the name of the duty of apoliticism to which they are subject as future officers. Our thesis is that strengthening *critical thinking* in the education provided to officer cadets at military academies is undoubtedly one of the best ways to guard against the dangers posed by political polarization for the officer profession. Critical thinking carries with it the potential to defuse some of the mechanisms at the heart of polarization, while also allowing for a critical look at the excesses associated with this all-encompassing phenomenon.

Keywords: critical thinking, political polarization, officers' education, officers' apoliticism

MATIAS FERREYRA WACHHOLTZ*
RENE MOELKER[2]

CULTURAL AWARENESS AND INTEROPERABILITY IN PEACE OPERATIONS

*Radboud University, [2]Netherlands Defence Academy

Contemporary peace and stability operations require military personnel to work across cultural, institutional, and professional differences in interagency environments. However, discussions on interoperability often emphasize technical and procedural dimensions, while giving less attention to the role of professional military education in developing cultural awareness and human interoperability. This paper examines connections between professional military education and interoperability in peace operations. The study is part of the Marie Skłodowska-Curie project "Knowledge Management and Models of Interoperability in Peace Operations" (MAMIP), conducted at Radboud University in cooperation with the Netherlands Defence Academy. The research draws on qualitative interviews and documentary analysis in military peace operations training institutions in the Netherlands and Brazil.

Keywords: interoperability, knowledge, PME

HANNA FORSBERG*
ØRJAN ROGNE RISE[2]

CULTIVATING HYBRID INTELLIGENCE: THE EDUCATIONAL IMPACT OF AI EXPLORATION IN MILITARY PLANNING

*Swedish Defence University, [2]Norwegian Defence University College

The rapid integration of Artificial Intelligence (AI) into military operations necessitates a critical examination of its impact on professional military education (PME). This paper presents findings from one of several study areas of the Comprehensive Shield 2026 (CS26) experiment, in which we investigated the pedagogical implications of an AI-based Decision Support System (DSS) in NATO-style operational planning exercises. Utilizing the ISAR (Inversion, Substitution, Augmentation, Redefinition) framework and Kirkpatrick's model for training evaluation, the research examines how the exploration of AI tools in operational practice influences learning experiences, cognitive load, and the development of higher-order skills among senior student officers.

Initially, the AI-DSS posed risks of cognitive disengagement (Inversion) and was operated at a basic Substitution level, leading to high cognitive load and a possible overreliance on AI outputs. However, with structured familiarization, its role predominantly evolved into that of a cognitive partner capable of fostering deeper learning (Augmentation). This shift enabled critical thinking and creativity, as students learned to rigorously validate, interpret, and creatively apply AI outputs, moving towards a "human-driven, AI-assisted" workflow. The study highlights essential domain competencies for AI-enabled military planning, including doctrinal proficiency, technical literacy, as well as crucial transversal skills like critical validation, collaboration, and adaptability.

These insights directly demonstrate how military technology adapts within educational curricula. The findings underscore that while initial challenges exist, AI can enhance military education on operations, preparing officers to leverage advanced technologies while maintaining human oversight.

Keywords: PME, artificial intelligence, operational planning, ISAR framework, critical thinking

ALEKSANDAR GRIZHEV*
VESNA POPOSKA[2], LJUPCO SOSOLOVSKI[3]

FROM OPERATIONAL INSIGHT TO INSTITUTIONAL ADAPTATION: INTEGRATING HYBRID THREAT LESSONS INTO PROFESSIONAL MILITARY EDUCATION

*-[3]Goce Delcev University

Hybrid threats have made adaptation one of the central challenges for contemporary military institutions. Recent conflicts have produced many useful operational insights, yet their translation into doctrine, training, and Professional Military Education (PME) is not always systematic enough. This gap is particularly visible in areas where hybrid competition affects not only the battlefield, but also the information environment, societal resilience, leadership, and decision-making.

This paper examines how lessons from hybrid threat environments can be better integrated into PME. It focuses on three areas where military education needs closer alignment with operational reality: understanding and operating in the information environment, including Foreign Information Manipulation and Interference (FIMI); preparing leaders to make decisions under ambiguity and cognitive pressure; and integrating societal and cross-cultural dimensions into military learning.

The paper uses a qualitative, analytical approach, combining a review of concepts on lessons learned, adaptation, and military education with analysis of contemporary hybrid-threat challenges. The OODA loop is used as an analytical lens to frame adaptation as a continuous process of observing operational change, orienting institutional understanding, deciding on educational priorities, and acting through adjustments to education and training.

The paper proposes a simple three-level model for adapting PME: updating key concepts, strengthening practical learning, and improving feedback among operations, doctrine, and education. The aim is to make military education more responsive to real operational challenges. In this sense, PME is not only a place where officers learn existing knowledge, but also a mechanism through which armed forces adapt, innovate, and prepare for future hybrid environments.

Keywords: hybrid threats, PME, lessons learned, information environment

ROBERT HILLIARD*
DANIEL PACKHAM[2]

ALTERNATE, ADAPTED, AND EMERGING: NEW EDUCATION AND TRAINING PATHWAYS TO OFFICERSHIP IN SWEDEN (AND UKRAINE).

*-[2]Swedish Defence University

Contemporary conflicts and challenges have led to innovations and adaptations for initial officer education and training. In this context, understanding what new pathways to Officership have emerged, how they differ from more mainstream pathways, and how they compare to other approaches can help shape future officer education and training. As part of a broader project on Swedish command supply – recruitment, education and training as well as retention – researchers have focused on “SOFU” (Special Officer Education and Training).

SOFU is a relatively new and evolving, shorter pathway for university graduates compared to the three-year mainstream academy programme. So far, it has enabled the retention and promotion of talented NCOs in more tactical roles and the recruitment of officers with important technical skills and specific staff/headquarters abilities. SOFU was established in 2018, recently expanded to include partnerships with new universities, and is under review and revision for 2027.

The project has produced research comparing a SOFU pathway with the UK “Sandhurst model” with an emphasis on infantry officers and a broader pilot interview study with SOFU graduates.

Both elements of this research have highlighted themes related to critical thinking.

This presentation will draw together selected findings from this ongoing research project, focusing on technology, innovation, adaptation, and lessons learnt that are evident in this alternate initial officer education and training option in Sweden. Findings on the origins, development, and extent of critical thinking will be a particular focus. In turn and based on the future direction for the SOFU element of this project, emerging findings linked to scoping work on Ukrainian National Guard initial officer education will add a new layer, and opportunities to explore our proposed research design.

Keywords: initial officer education & training, Sweden, Ukraine

PATRICK HOFSTETTER*

MORE MILITARY. MORE ACADEMY: RESEARCH-BASED TALENT DEVELOPMENT IN PROFESSIONAL MILITARY EDUCATION

*Military Academy at ETH Zurich and Swiss Armed Forces

Military academies are often situated between the demands of practical training and academic education – a debate commonly referred to as the 'Sparta versus Athens' dichotomy. The accelerating pace of technological change further intensifies this tension, as officers must combine military practice with technological and scientific reflection at an earlier stage. At the same time, military-related academic research has become more difficult because technological innovation has increasingly been driven by civilian institutions, and parts of the European higher education system have grown more distant from the military in recent decades.

This article examines how research-based professional military education (PME) can serve as a bridge: Its aim is not only to prepare junior officers for dealing with emerging technologies and research, but also to align research fields more closely with military practice.

Using the Military Academy at ETH Zurich as a case study, this article demonstrates how such education can take place at the Bachelor's level. This benefits from the distinctive nature of Swiss PME, where students at the Military Academy already possess several years of command experience at platoon or even company level before beginning their studies. The case study details how, over the past three years, a total of 13 students were selected and mentored in submitting papers or posters to suitable conferences. Three projects further illustrate how this led to follow-on research and innovation initiatives.

As part of a qualitative study, seven semi-structured interviews were conducted to examine prerequisites, perceived relevance, self-efficacy, and perceived transferability. The study reaches the preliminary conclusion that the chosen approach represents a potentially transferable framework for developing young military talent. It identifies necessary and facilitating conditions, as well as opportunities and risks. The article concludes that the future of military academies is not a choice between Sparta and Athens, but requires more of both: more military and more academy.

Keywords: PME, officer education, military academies, talent development, research

TAAVI LAANEPERE*

TRAINING FOR LARGE-SCALE WAR AND MILITARY EFFECTIVENESS IN COMPARATIVE HISTORICAL PERSPECTIVE

*Estonian Military Academy

The return of high-intensity interstate war in Europe has renewed attention to how armed forces prepare for large-scale conflict. This presentation examines historical models of military training and professional military education in the context of preparing armed forces for prolonged, high-intensity war. Using comparative historical analysis, the study analyses three cases: the First World War, the Finnish Winter War (1939–1940), and the Second World War.

The presentation addresses two questions: what types of training and military education systems have been used to prepare for large-scale war, and through which mechanisms do these systems influence military effectiveness and the moral dimension of warfare.

The findings show that the effects of training systems are mediated through organizational and moral mechanisms rather than through training practices alone. Comparative analysis identifies four interconnected conditions that shape military effectiveness: leadership practices and leader development; institutional learning and training adaptation; the formation of unit cohesion and moral readiness; and the alignment between peacetime training, reserve systems, and wartime force generation. The study further argues that war duration constitutes a critical analytical dimension: mechanisms supporting initial readiness do not necessarily sustain long-term effectiveness in prolonged conflict.

By integrating comparative historical analysis with the RAND ‘will to fight’ framework, the presentation conceptualizes training systems as strategic institutional capabilities through which organizational structures, leadership, cohesion, and morale are translated into sustained military effectiveness.

Keywords: military training systems, military effectiveness, will to fight, institutional learning, large-scale conventional war

ANDREW HOCK CHYE LIM*

TECHNOLOGY ENABLED LEARNING TO DEVELOP STRATEGIC APPRECIATION: DESIGN, EXECUTION, AND ANALYTICAL FINDINGS IN EDUCATING MID-CAREER OFFICERS

*SAFTI Military Institute - Singapore Armed Forces

As military environments grow increasingly complex, Professional Military Education must continually refine its pedagogical frameworks. A critical challenge is developing the strategic appreciation competency necessary to transition mid-career officers from tactical operators to operational and strategic thinkers.

This presentation details the design, execution, and empirical findings of a Technology-Enabled Learning intervention implemented at the Goh Keng Swee Command and Staff College.

Advances in learning technologies and enhanced pedagogies now enable personalized, data informed education to support diverse abilities. Leveraging the iLEARN platform, the college adopted a flipped classroom model using online self-directed content to build foundational knowledge, followed by face-to-face sessions for higher-order application. Using aggregate conscious competence matrix data from iLEARN, educators measure pedagogical efficacy and evaluate progress across five components: Definition, Purpose, Strategic Frame, PMESII (Political, Military, Economic, Social, Information, and Infrastructure), and DIME (Diplomatic, Informational, Military, and Economic).

Analytics identify where persistent cognitive friction occurs. Learners demonstrate challenges applying PMESII and DIME concepts to complex scenarios, specifically mapping multiple actor interactions amidst hybrid conflict ambiguity. These gaps are addressed during face-to-face sessions, where educators provide context and define effects when placing variables within PMESII to frame problems and DIME to resolve issues. Integrating interactive panels transforms the learning dynamic from passive reception to active participation, allowing the exchange of ideas to deepen comprehension.

These findings underscore that while foundational modules prime baseline knowledge, bridging the gap between principles and practical application requires further pedagogical evolution. The presentation concludes by outlining recommendations for curriculum enhancement, integrating wargaming to reinforce the cognitive agility required for military command in contested operational environments.

Keywords: technology-enabled learning, strategic appreciation, PME, learning analytics, cognitive agility

ROBERT LUMMACK*

UAS CAPABILITY DEVELOPMENT: TRENDS, REALITIES AND TRAINING NEEDS FOR IMPACTFUL ALLOCATION

*Non-Commissioned Member Leadership College

The war in Ukraine and geopolitical competition have prompted re-evaluations of military preparedness and force generation globally (SIPRI 2026). The need to convince governments and publics to increase defence investment, a dominant narrative since 2014, has now shifted to questions of allocation and prioritization – where and how to invest? Critically, the opportunity cost of expenditure on ineffective or irrelevant capability/means looms as significant societal and military risks. This paper focuses singularly on the burgeoning issue of drones, or Unmanned Aircraft Systems (UAS), platforms that many militaries desire to augment to ensure contemporary warfighting relevance. This desire is logical given the visibility and importance of UAS within the war in Ukraine. However, due to the emergent and rapid nature of UAS development, there is a need for an iterative and continued understanding to inform acquisition and training efforts. Part one examines force employment trends from Ukraine and Iran, considering offensive and defensive aspects of UAS. Part two examines the state of the UAS industry globally, examining technological developments, market leadership, and manufacturing realities. Finally, part three examines the implications of UAS developments on military training systems. The overall argument is that UAS development should aim to be sustainable, scalable for mass and adaptable to diverse and potentially unknown operational needs. Data sources include combatant experiences, global production data, analyses from think tanks and national case studies. Multinational and multilevel sources are used to ensure a broad analysis, useful to inform ongoing and impending national discussions about UAS investment.

SIPRI. (2026, April 27). Global military spending rise continues as European and Asian expenditures surge. SIPRI. https://www.sipri.org/media/press-release/2026/global-military-spending-risecontinues-european-and-asian-expenditures-surge

Keywords: UAS, drones, force employment, force generation, training

HEMANT MALHOTRA*

BEYOND THE TEXTBOOK: ADAPTING MILITARY EDUCATION FOR AI-ASSISTED HYBRID THREATS

*School of International Studies, Indira Gandhi National Open University (IGNOU), New Delhi, India

The proliferation of artificial intelligence (AI) in hybrid warfare has created an unprecedented gap between threat evolution and military education response. While AI-assisted hybrid threats operate at machine speed, professional military education (PME) continues to move at human speed, with only 10–15% of personnel feeling adequately prepared for AI-enabled adversaries.

This paper analyses AI integration programmes across 11 countries, reviews NATO and EU education frameworks, and examines India's PME system to identify barriers to curriculum reform. The study synthesises doctrinal literature, policy documents, and comparative institutional analysis to develop an actionable adaptation framework.

The findings reveal that AI amplifies hybrid threats across all domains: deepfake incidents increased fivefold since 2019, with 191 distinct AI-driven information operations recorded in Ukraine between 2022 and 2024. The US Army Command and General Staff College's AI-enabled wargaming achieved a fivefold increase in throughput for decision-cycle training. India's PME faces distinctive structural constraints: 44% of the defence education budget is allocated to salaries, and the National Defence University remains non-operational after more than 15 years. The paper proposes a five-pillar curriculum framework: AI Literacy, Hybrid Threat Recognition, Cognitive Resilience, Ethical Decision-Making, and Continuous Adaptive Learning. Faculty development emerges as the critical bottleneck, requiring 20–25% of budget allocation.

This paper offers the first integrated curriculum adaptation framework that bridges AI threat analysis with a concrete Indian reform roadmap, providing both theoretical scaffolding and practical policy guidance for PME institutions worldwide.

Keywords: military education, artificial intelligence, hybrid threats, curriculum reform, professional military education, deepfakes, disinformation, cognitive warfare, India, NATO

RONALD MAÑEJE*

INSTITUTIONALIZING STRATEGIC THINKING IN THE PHILIPPINE MILITARY ACADEMY THROUGH MIND SPORTS INTEGRATION

*

The contemporary security environment is increasingly characterized by hybrid warfare, gray-zone operations, cyber threats, and complex multi-domain engagements. These developments require military leaders who possess not only tactical proficiency but also advanced cognitive capabilities such as strategic foresight, adaptability, and decision-making under uncertainty. While the Philippine Military Academy (PMA) remains the premier institution for officer development in the Armed Forces of the Philippines (AFP), its current training framework lacks a structured system for developing higher-order strategic thinking skills.

This study proposes the institutional integration of mind sports – such as chess, Go (Weiqi/Baduk), and similar strategic games – into PMA's leadership development program. These disciplines are globally recognized for enhancing cognitive functions critical to military operations, including pattern recognition, probabilistic reasoning, and long-term strategic planning.

Using a mixed-method research design and the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) framework, this study identifies capability gaps in PMA's cognitive training system. It then proposes the establishment of a Strategic Thinking Development Program (STDP), which integrates mind sports into the academy's curriculum and training structure.

The study concludes that institutionalizing mind sports will significantly enhance the strategic competence of future AFP officers, contributing to a more agile, adaptive, and intellectually competitive force aligned with national defense priorities

Keywords: strategic thinking, mind-sport, military education, military training

ISAAC MOFOKENG*

ASSESSING THE RELATIONSHIP BETWEEN DIGITAL FINANCIAL LITERACY AND FINANCIAL WELL-BEING AMONG RECRUITS IN THE MILITARY SKILLS DEVELOPMENT SYSTEMS (MSDS)

*Stellenbosh University (Faculty of Military Science)

Global uncertainties, including those exacerbated by the COVID-19 pandemic, have highlighted the vulnerability of young adults to financial instability, particularly those entering the workforce with limited financial experience and education. This vulnerability is particularly pronounced among young adults in structured, high-pressure environments, such as the South African National Defence Force (SANDF), where they face unique challenges, including frequent relocations, limited spending opportunities, predatory lending, and reliance on digital financial services (DFS) during remote deployments.

Driven by rapid growth in digital finance, mobile banking, and digital wallet adoption in South Africa has exceeded 60%, making digital financial literacy (DFL) essential for safely navigating DFS among young adults who rely heavily on digital platforms. This study aims to assess the effect of digital financial literacy on financial well-being among recruits in the Military Skills Development Systems (MSDS). Using a cross-sectional quantitative approach, data were gathered through a self-administered questionnaire among a convenience sample of recruits.

The findings revealed a moderate, statistically significant positive relationship between DFL and FWB, as determined using SPSS. The study underscores the need for tailored, evidence-based financial literacy interventions within the SANDF that prioritise digital competencies. Such programs could improve recruits' financial decision-making, long-term stability, operational readiness, and ultimately national security

Keywords: digital financial literacy, financial well-being, financial education

NEERAJ*

THINKING BEYOND THE BATTLEFIELD: OFFICER DEVELOPMENT IN THE AGE OF MULTI-DOMAIN OPERATIONS, HYBRID WARFARE, AND RAPID TECHNOLOGICAL CHANGE

*Panjab University

Modern warfare has changed dramatically. Conflicts are no longer fought only on land, sea, or air but simultaneously across physical battlefields, cyberspace, outer space, and the information environment, which can be called multi-domain operations. Adversaries increasingly combine force, disinformation, economic pressure, and political manipulation, an approach known as hybrid warfare. Technology is changing so rapidly that it's hard to find solutions in an equally short time.

Officer training has traditionally focused on tactical skill and procedure. These remain valuable but are no longer sufficient as officers face situations with no clear enemy, no defined battlefield, and no rulebook for the decision at hand. Military judgment has long concerned military organisations, mainly through command psychology and stress-based decision-making. This paper's contribution is different: it shows that technological modernisation and judgement development are advancing at unequal speed and argues that this gap, not technology itself, is the central risk in future conflict.

This paper examines two Indian cases. *Operation Sindoor* in May 2025 was India's first military operation to formally synchronise cyber, drone, space, and information warfare, and required officers to make real-time judgement calls under jamming, disrupted drone identification, and an active disinformation campaign, while political leadership balanced precision strikes against escalation control. Along the *Line of Actual Control* with China, sustained grey-zone tactics, including disinformation, economic pressure, and gradual territorial pressure, have tested Indian officers' ability to read intent and respond without triggering open conflict.

Drawing on open-source military analysis, official statements, and existing scholarship, this paper argues that human judgment, educated, reflective, and ethically grounded, remains the most decisive factor in multi-domain and hybrid conflict and developing it must become the central purpose of officer education worldwide.

Keywords: military education, officer training, hybrid warfare

AMER RIKOVIC*

LEARNING HOW TO OPERATE TOGETHER

*Ministry of Defence & HQ SACT ToE

This article examines Quality Assurance (QA) within NATO's Education and Individual Training (E&IT) system as a central governance instrument underpinning Alliance readiness, multinational interoperability, and institutional transformation. Drawing on qualitative analysis grounded in doctrinal review and conceptual synthesis, the study explores how NATO ensures that validated operational requirements are systematically translated into measurable learning outcomes in a multinational environment. Particular attention is given to the NATO Global Programming System (GPS) and the Systems Approach to Training (SAT), which function as mutually reinforcing processes that convert strategic intent into coherent and adaptive education and training solutions. The article offers an interpretive perspective relevant to practitioners and scholars in defense education.

Keywords: quality assurance, NATO education and training, systems approach to training, Global Programming System, interoperability

JILL SCOTT*
CECILE MALARDIER-JUGROOT[2]

RAPID RESPONSE IN SUPPORT OF NATIONAL SOVEREIGNTY: ACCELERATING RESEARCH AND INNOVATION FOR DEFENCE CAPABILITIES AT THE ROYAL MILITARY COLLEGE OF CANADA

*-[2]Royal Military College of Canada

Rapid response and urgent action does not always characterize change at universities. But threats to Canada's national sovereignty have sharpened attention to the need to immediately accelerate defence research and innovation at the Royal Military College of Canada (RMC). In June 2025, the Minister of National Defence introduced the BOREALIS program, an innovation coordination mechanism to accelerate the development of new defence and security capabilities by connecting government, academia, industry, and the military. In February 2026, Canada's first Defence Industrial Strategy was announced, a policy framework that puts research, innovation, and economic growth at the centre of its approach to bridge the longstanding gap between Canada's research excellence and its defence capabilities. Our paper will highlight how RMC is uniquely placed to respond to these policy announcements and outline the initiatives currently underway.

Celebrating its 150th anniversary in 2026, RMC is one of two defence universities in Canada with a core mission to educate officers for the Canadian Armed Forces. What is less visible is RMC's vibrant research enterprise with its unique capabilities in a variety of defence and security-related fields, including uncrewed vehicles, permafrost, and northern infrastructure, remote sensing, cybersecurity, electronic warfare, and defence policy and security intelligence, to name only a few. While RMC is a small university with limited capacity, it is a sovereign resource with longstanding research partnerships with a multitude of CAF units. By partnering with civilian universities and Canadian companies, RMC has an important role to play in workforce development as well as accelerating, expanding, and facilitating innovations to contribute to defence capabilities.

Our paper will highlight both the opportunities and the challenges of rapidly expanding and accelerating RMC's research and innovation enterprise. We will reference other models, including Nordic approaches to Total Defence and Comprehensive Security.

Keywords: defence research, innovation ecosystems, military capabilities

KHALID SHAFI*
JENS MATHIESEN[2]

FROM THE ARCTIC TO THE THIRD POLE: CLIMATE SECURITY, STRATEGIC FORESIGHT, AND PROFESSIONAL MILITARY EDUCATION

*NDU, Pakistan, Institute of Strategic Studies, Research and Analysis, [2]RDDC

Climate change is increasingly reshaping the security environment by affecting water security, disaster risk, governance capacity, migration, and regional stability. For military professionals, these changes require more than operational preparedness; they also demand critical thinking, strategic foresight, and the ability to understand complex, interconnected risks. This paper examines the Hindu Kush-Himalaya region, commonly referred to as the "Third Pole", as a strategic climate security case for professional military education.

The central research question is: How can the Third Pole be used within military education to strengthen strategic foresight and interdisciplinary thinking among military professionals? The paper adopts a qualitative comparative approach, using the Arctic as a reference case and the Third Pole as the main pedagogical case. The evidence base includes climate-security scholarship, comparative regional governance literature, policy documents, and the United Nations Climate Security Mechanism.

The analysis is guided by three dimensions: environmental stress, regional governance, and military learning. The Arctic, despite strategic competition, has benefited from institutionalized dialogue and scientific cooperation through the Arctic Council. In contrast, the Third Pole supports the water security and livelihoods of more than a quarter of the world's population and connects politically sensitive and militarized spaces, including three nuclear-armed states, yet lacks a comparable regional platform for addressing shared environmental risks.

The paper argues that the Third Pole can help military students move beyond traditional threat centric thinking toward broader environmental-security analysis. It proposes the conceptual foundations of a South Asian Climate Security Mechanism as a classroom and policy-oriented framework for examining regional learning, disaster preparedness, confidence-building, and strategic dialogue. The paper contributes to military education by showing how climate-security cases can cultivate anticipatory judgment, reflective thinking, and strategic adaptability in uncertain security environments.

Keywords: PME, climate security, Third Pole, strategic foresight

ASKIN INCI SOKMEN ALACA*

HUMAN–MACHINE TEAMING AND COGNITIVE AUGMENTATION IN FUTURE WARFARE: MILITARY IMPLICATIONS OF NEURAL INTERFACES AND IMMERSIVE TRAINING ENVIRONMENTS

*Global Defense Information Center

Contemporary warfare increasingly requires military personnel to operate within data-saturated, cognitively contested, and technologically accelerated environments shaped by artificial intelligence, autonomous systems, cyber operations, and multi-domain warfare. In this context, traditional military training and decision-making structures may become insufficient for future operational complexity.

This paper explores how emerging forms of human-machine teaming could evolve toward cognitive augmentation through neural interfaces, adaptive learning systems, immersive simulations, and holographic metaverse-based military training environments. Drawing on developments in neurotechnology, AI-assisted cognition, extended reality (XR), and military innovation studies, the research examines how future armed forces may integrate immersive digital ecosystems into operational readiness and military education.

The study focuses on speculative, yet increasingly relevant concepts such as accelerated skill acquisition, neural feedback systems, synthetic memory support, and persistent virtual training environments inspired by military futurism and science-fiction-informed strategic thinking. While technologies associated with “mind uploading” remain theoretical, adjacent developments in brain-computer interfaces and cognitive enhancement already influence defence research agendas and strategic foresight discussions.

The paper addresses three research questions: (1) How could cognitive augmentation technologies transform military training and operational effectiveness? (2) What role might immersive metaverse-based simulations play in multi-domain operations? (3) How can military institutions balance the operational advantages of neural integration technologies with ethical and strategic constraints?

Using a qualitative and interdisciplinary methodology, the study combines military innovation literature, cognitive warfare studies, neuro-ethics, posthuman security studies, and scenario-based strategic foresight analysis. The paper argues that future military effectiveness may increasingly depend on cognitive superiority and human-machine integration rather than solely on kinetic capabilities.

Keywords: human–machine teaming, cognitive augmentation, neurotechnology, XR Training, metaverse warfare

ANDERS MCD SOOKERMANY*
THOMAS SLENSVIK[2]

FROM FRICTION TO TRACTION: DESIGNING EPISTEMIC SPACE FOR INNOVATION IN PROFESSIONAL MILITARY EDUCATION

*Norwegian Defence University College, [2]Norwegian Defence University College, Command and Staff College

Professional military education is increasingly expected to prepare officers for complex operational environments in which doctrines, planning procedures, and technological tools remain necessary, but may not provide sufficient orientation on their own. This paper explores how pedagogical interventions in joint operational planning education may help students attend to and reconfigure the epistemic space within which situations become intelligible, possible futures thinkable, and action possible.

The paper draws on an ongoing practice-based research programme across courses in operational art, military strategy, joint operations, and the *Comprehensive Shield* exercise at the Norwegian Defence University College. The material includes observations, interviews, reflective fieldnotes, audio recordings, and student-produced planning artefacts collected across successive educational iterations.

Drawing on Sevaldson's Systems Oriented Design, Gibson's concept of affordances, and De Matteis' development of affective and relational affordances, the paper approaches SOD not primarily as a method, but as a systemic orientation toward complexity enacted through situated design practices. We propose the distinction between *friction* and *traction* as an analytic contribution. Friction refers to interventions that interrupt taken-for-granted assumptions, habitual planning routines, and premature closure. Such interventions can bring into view tensions among doctrinal formulations, planning formats, and the complex situations students are asked to engage with. Traction refers to students' collective development of a provisional but workable foothold: a capacity to sustain inquiry and act meaningfully without experiencing uncertainty as a loss of direction or a slide into chaos, while also resisting premature resolution through the reduction of complexity.

Preliminary observations suggest that innovative planning practices emerge through changing relations among facilitation, doctrinal formats, material artefacts, and students' own participation. It contributes by showing how professional military education may cultivate collective capacities for perceiving, questioning, and working with complexity in ways that support innovation.

Keywords: PME, epistemic space, Systems Oriented Design, joint operational planning, complexity

ÜLLE SÄÄLIK*

DEVELOPING MILITARY LEADERS: GROWTH, SHIFT, OR FLUCTUATION IN LEADERSHIP IDENTITY?

*Estonian Military Academy

During professional education and preparation for a new role, individuals begin to compare their current self-concept with possible and ideal future selves (van Knippenberg et al. 2004: 828). Research suggests that leaders tend to embody the ideal standards of their group (Hogg & Vaughan 2002: 321). Consequently, individuals undergoing military leadership training may experience considerable pressure to conform to idealised leadership expectations. At the same time, leadership literature indicates that leaders perceived as authentic by their followers are more likely to empower their subordinates and contribute to higher levels of job satisfaction (e.g. Wong & Laschinger 2013). However, striving excessively to project an idealised image may conflict with perceptions of authenticity.

The present study examines how officer cadets and master's degree students at the Estonian Military Academy perceive themselves at the beginning of their studies and how these perceptions evolve over time. Specifically, the study seeks to determine whether changes in self-perceived military leadership competencies reflect developmental growth (i.e. progression from lower to higher competency levels), a shift in the nature of self-perception, or irregular variation in competency assessments. Furthermore, the study investigates which competencies are regarded as most important at the outset of the educational programme.

Changes in military leadership identity were examined through the lens of leadership competencies using the MILTIC model (Säälik et al. 2020; Säälik 2022).

Students at the Estonian Military Academy completed a military leadership competency questionnaire on at least three occasions during their studies. Changes in self-assessments were analysed using descriptive statistics, including measures of central tendency and variation. The results indicate initially high self-assessment scores, supporting the assumption of an idealised self-view at the beginning of professional military education. More detailed patterns and findings will be presented in the paper.

Keywords: military leaders, professional identity, self-assessment

INGVILD TEGNANDER*

NEGOTIATING PROFESSIONAL IDENTITY THROUGH FEEDBACK IN MILITARY LEADER EDUCATION IN NORWAY

*The Norwegian Defence University College

This work-in-progress examines how professional officer identity in the Norwegian Military Academy is negotiated and constructed through feedback practices. Through semi-structured interviews and participant observation with two cadet teams during their first year at the Military Academy, three registers of feedback have been identified: (1) structured sessions organised around an institutional formula, (2) direct peer exchanges outside formal settings, and (3) normative commentary (remarks and interactions not framed as feedback, but that still communicate expectations and regulate conduct). A particular focus is this third register, where humour, informal exchanges, reactions, and shared language seem to have a significant effect on how the cadets subtly shape each other and themselves into what they perceive to be the optimal officer. Another central empirical observation is that cadets draw heavily on the language of trust (tillit), mobilising, negotiating, and withholding it to assess and produce each other as credible officers-in-formation. The data further show that trust language is largely absent from feedback sessions conducted before the field exercise and becomes pervasive after it, suggesting that the exercise functions as a threshold through which professional values become operative and nameable. The article contributes to research on professional identity formation in military education by showing how cadets are simultaneously active agents in this process and subjects shaped by an institutional structure of self-examination and peer judgement that they did not design.

Keywords: military education, officer identity, professional military identity, discourse

RONALD TI*

OPERATIONAL LOGISTICS: PME'S UGLY DUCKLING

*King's College London

This presentation will discuss the current state of military logistics teaching at most joint staff courses, briefly remind/ highlight the criticality of logistics to warfighting and deterrence, and present a (suggested) generic 4-session course in operational logistics that could be applied to address this established PME knowledge gap at the joint staff course level. The presentation will draw on the speaker's experience in a number of NATO and EU PME establishments over the past decade. The speaker does not argue that logistics will suddenly become interesting, but rather that the majority of disinterested joint course students should have more than a passing knowledge of logistics and how it applies to the comprehensive operations planning process. It is better to learn this in the classroom than on first contact with the enemy! This presentation will close by describing how wargaming can be used to teach operations logistics, based on the speaker's 2023 PhD research in Estonia.

Keywords: operational logistics, military education, logistic wargaming

JUVENCIO ANTONIO VASCONCELOS LOBO*

MILITARY EDUCATION AND THE ENVIRONMENT: INSTITUTIONAL CONCEPTIONS IN THE BRAZILIAN ARMY (2014-2022)

*Meira Mattos Institute and Army Command and General Staff College

As extreme climate events intensify, the Armed Forces are increasingly mobilized for environmental crises, making them central actors in public policy and necessitating a critical investigation into military education concerning environmental governance. This study addresses the core research question: What conceptions of the environment are present in the official Course Plans (PLADIS) of the Brazilian Army's higher education institutions between 2014 and 2022? Methodologically, a qualitative documentary analysis was conducted on 216 Course Plans across the three main pillars of an officer's career: AMAN (tactical), EsAO (operational), and ECEME (strategic). The research examines the formalized curriculum through pedagogical indicators, framing the Army as a "total institution" (Goffman) to analyze how it projects an institutional "view" (Merleau-Ponty) onto reality. The analysis reveals three major findings. First, the prevailing framework is dominated by a technocentric conservationism tied to national-developmentalism, which conceives nature as an instrumental resource that ensures autonomy rather than as a global sanctuary. Second, this utilitarian conception evolves across ranks: changing from a physical obstacle or manoeuvre terrain at the tactical level (AMAN), to an administrative and legal liability at the operational level (EsAO), and finally to a geopolitical variable of sovereignty specifically concerning the Amazon at the strategic level (ECEME). Third, a profound "curricular silence" exists regarding climate change, suggesting institutional resistance to non-classical adaptation roles. The study concludes that while this educational model efficiently trains officers in environmental management, its silence on climate change leaves strategic leadership without a unified conceptual framework to address modern environmental insecurity.

Keywords: PME, curriculum analysis, environmental conception, Brazilian Army

SAMUEL ZILINCIK*
FAITH KLIJIAN[2]

COGNITIVE SUPERIORITY BEGINS WITH EMOTION SCIENCE LITERACY: THE CASE OF DOUBT

*-[2]Royal Danish Defence College

We argue that emotion science literacy, understood broadly as the awareness of the rapidly progressing study of emotions, should form an essential component of any meaningful effort to maintain cognitive superiority. Specifically, we propose that emotion science literacy contributes to better professional military education (PME), enables more effective military decision-making, and facilitates the development of more sensible military and strategic theories. To make our case, we review recent psychological research on emotions and the relevant research originating in security, strategic, and military studies. To illustrate the utility of emotion science literacy in military contexts, we conceptualize doubt as an emotion and deductively explore the practical implications of such conceptualization. While doubt is often viewed negatively by military professionals and theorists, treating it as an emotion enables us to break it down into its constitutive and manageable elements, thus highlighting its value in PME, military decision-making, and military/strategic thought development. Overall, our argument enriches the existing debate about cognitive superiority by directing attention to the role of emotions and provides guidance for how professionals and practitioners can gain an advantage over their adversaries by harnessing insights from the contemporary science of emotion.

Keywords: doubt, emotion, PME

ROUNDTABLES

ANNE MARIE HAGEN*
FRANCIS CLERMONT[2], KJETIL ENSTAD[3], ROLAND HELLBERG[4], OMHANI AMBRE NAIJA[5], DOROTA DOMALEWSKA[6], KATERINA VELJANOVSKA BLAZHEVSKA[7], PIOTR OKULSKI[8]

CRITICAL THINKING IN PME: COMPETENCE, DISPOSITION, OR CAPABILITY?

*,[3]Norwegian Defence University College, [2]Department of Professional Military Education, [4]Swedish Defence University, [5]Tunisian Military Academy, [6,8]War Studies University, [7]MIT University, Skopje

Critical thinking is one of the goals of higher professional military education on which there is near-universal agreement (Enstad & Hagen 2025). Yet, despite consensus on its importance, conceptions of critical thinking vary widely across military education systems. Critical thinking is variously regarded as a set of analytical tools or as academic reasoning skills, but it is rarely regarded in terms of autonomous thinking, despite this being an important component of this skillset (Antrobus & West 2022; Parenteau 2021). Nor do the dispositions that are key to developing critical thinking receive much sustained attention. As critical thinking is considered particularly relevant for managing the complexities and rapidly shifting dynamics of conflicts and warfare in the 21st century, it is crucial to investigate this concept further in the context of the military profession and how PME can support embedding it as a practice.

This roundtable brings together contributors to an edited collection on Critical Thinking in Professional Military Education to explore how critical thinking can be effectively cultivated, taught, and assessed across PME contexts. Drawing on work in progress, the panel will examine conceptualisations of critical thinking, pedagogical approaches, and institutional challenges, as well as the implications for officer development in an era shaped by hybrid threats, evolving battlefield dynamics, total defence scenarios, and technological developments that impact decision-making processes. By fostering dialogue between scholars and practitioners, the panel aims to connect ongoing research with broader ISMS concerns regarding the integration of operational insight, education, and defence innovation. It will highlight how PME can support more reflective, adaptive, and strategically minded professionals capable of navigating complex and evolving security environments.

Presentations within the Military Education Round Table:

1. Rethinking Critical Thinking in PME and Military Sciences: From the Paradigm of Simplicity to the Paradigm of Complexity
    - Francis Clermont (Department of Professional Military Education)
2. Visual Literacy as a Dimension of Critical Thinking in Professional Military Education: Visual Disinformation, Cognitive Warfare, and Pedagogical Implications
    - Dorota Domalewska (War Studies University, Poland),

   - Katerina Veljanovska Blazhevska (MIT University, the Republic of North Macedonia)
   - Piotr Okulski (War Studies University, Poland)
3. Messy Realities: Towards Critical Thinking as Situated Professional Judgement
   - Anne Marie Hagen (Norwegian Defence University College)
   - Kjetil Enstad (Norwegian Defence University College)
4. Cultivating Critical and Creative Thinking in Professional Military Doctoral Education
   - Roland Hellberg (Swedish Defence University)
5. Beyond Skills: Character Strengths as Dispositional Foundations of Critical Thinking in PME
   - Omhani Ambre Naija (Tunisian Military Academy) (Panel presentation by Naija)

Keywords: critical thinking, professional military education, pedagogy, higher professional education

WORKING GROUP 10:
STRATEGY

Chairs

JĀNIS BĒRZIŅŠ
National Defence Academy of Latvia

LUKAS MILEVSKI
Leiden University

Co-Chair

DUMITRU MINZARARI
Baltic Defence College

ÖZGENUR AKTAN*

THE DIALOGUE BETWEEN HEDGING AND NORDIC BALANCE IN SMALL STATE STRATEGY?

*Turkish National Defence University, Atatürk Strategic Studies and Graduate Institute (ATASAREN)

Hedging has been one of the most prominent small-state strategies in great power competition. The boundaries of this strategy have been quite flexible, encompassing a range of policies such as adopting active neutrality, avoiding both alignment and confrontation through noncommittal yet adaptable security policies, and embracing a middle ground approach among alignment, balancing, and bandwagoning to simultaneously establish relationships with great powers.

Consequently, this strategy requires complicated and sophisticated tactics in response to the threats and uncertainties, as well as great power competition, in the international system. Collectively, the Nordic countries – Denmark, Finland, Iceland, Norway, and Sweden – exhibited such patterns in their strategies that can be interpreted, to some extent, as the tactics of hedging, particularly through their differing security policies and multilateralism during the Cold War. This Nordic balance tradition elucidates how the diverse security policies and multilateralism of a distinctive group of small states can foster regional order and stability within the competitive and loosely bipolar system. Set against this backdrop, this paper investigates how hedging and the Nordic balance address and conceptualize regional order and stability in the security policies of small states. In doing so, it sheds light on their converging and diverging aspects. With a dialogue between hedging and the Nordic balance, this paper scrutinizes the complementary relevance of the Nordic balance tradition for the hedging strategies and its theoretical contributions, given the conceptual expansions and limitations of hedging. As a result of this synthesis, the paper argues that while hedging strategies primarily revolve around small states' efforts to manage threats and uncertainties, there is less theoretical emphasis on regional order and stability as an outcome of small states' interactions. In response, the Nordic balance tradition offers complementary insights into how regional order and stability can emerge from the interactions of small states, thereby contributing to a regionally constituted zone of security.

Keywords: hedging, Nordic balance, Nordic countries, small states, strategy

JĀNIS BĒRZIŅŠ*

RUSSIA'S DRONE WAR IS NOT ABOUT DRONES

*National Defence Academy of Latvia

In 2025, Russia activated a dedicated branch of its armed forces for unmanned systems. Drawing on Russian-language primary sources from *Armeyskiy Sbornik* and *Voyennaya Mysl'*, journals that have received almost no attention in Western analysis, this article argues that the significance of drone warfare lies not in the platforms themselves but in the operational system being assembled around them. Russian military authors have codified six tactical engagement contours, each a closed sensor-to-shooter loop operating at the battalion level. A separate cost-effectiveness model demonstrates that expendability becomes the rational procurement choice once per-sortie loss rates exceed roughly 25%. The hardware reflects this logic. Carbon fiber has given way to polyethylene pipes and command infrastructure runs on commercial smartphones over 4G networks. Ukraine, with no coordination with Russia, has arrived at a near-identical architecture: dedicated unmanned branches, expendability as the governing procurement logic, organic drone integration down to battalion level, practice outpacing formal doctrine in both cases. This convergence, not the drone itself, is the signal of structural change. The architecture is already diffusing beyond the Russia-Ukraine theater. Insurgents in Myanmar download Ukrainian flight simulators via Telegram. Hamas has used drones to blind Israeli checkpoints. Chinese civilian drone patents account for over 70% of the global total. The temptation to dismiss this as a poor man's war collapses against the fact that NATO spent $1.36 trillion on defense in 2023, 12 times Russia's budget, with a substantial share directed toward unmanned systems, while Britain's 2025 Strategic Defence Review envisions ground forces that are 80% unmanned. The contour system closes kill chains at the battalion level in minutes, below the threshold at which many NATO command structures operate. The central question for Western armies is not whether to acquire drones but how to decentralize command authority to where they fight.

Keywords: Drones, Russia, NATO

JUN YAN CHANG*
ADRIAN U-JIN ANG[2]

A FRIEND IN NEED IS A FRIEND INDEED: THE UNITED STATES AND ITS JOINT MILITARY EXERCISES IN THE ASIA-PACIFIC

*-[2]Nanyang Technological University, S. Rajaratnam School of International Studies

Multilateral or joint military exercises have become more prevalent, especially with the so-called "return of geopolitics" as well as rising United States-China competition amidst a more complex security environment. Today, only a handful of states within the international system have not participated in any joint military exercise. Nevertheless, despite the proliferation of such multilateral exercises, the phenomenon remains little studied. Evidently, they are more than just mere training programmes. Within the relevant, though limited, literature, there are two other main explanations for joint military exercises: deterrence and defence diplomacy. We contend, however, that joint military exercises serve both purposes concurrently, thereby contributing equally to regional order, albeit in different forms. Indeed, following Ang, Chang and Loo (2025), "the key material indicators" of such exercises, "their scale and type", fail to even "allow us to distinguish between their deterrence and defence diplomacy functions". We test our claim with reference to US joint military exercises in the Asia-Pacific. In this manner, this paper further accounts for the US role in the region's international order.

Keywords: joint military exercises, deterrence, defence diplomacy, international order

EDMUND CURRY*

STRATEGIC AGENCY UNDER DURESS: LESSONS FROM THE WINTER WAR FOR SMALL STATES

*United States Military Academy

In 1939, Finland chose resistance over subordination when faced with Soviet demands. In doing so, the ensuing "Winter War" provides a useful model for contemporary small states confronting great powers. First, small states should employ a defense-by-denial strategy. Second, they must offset conventional disadvantages by converting commercially available technologies into scalable, low-cost military capabilities. Third, whole-of-society mobilization is required to maximize the costs small states impose.

During the Winter War, Finland confronted overwhelming Soviet advantages in manpower, armor, and industrial capacity. Rather than seeking conventional parity, Finnish forces pursued a denial strategy designed to raise the costs of conquest. This logic reflects contemporary "Porcupine" concepts, including Taiwan's defense strategy and Ukraine's resistance against Russia, both of which prioritize survivability and the ability to make aggression prohibitively costly rather than achieving battlefield dominance.

The second key element of Finland's success was its ability to rapidly militarize civilian resources. Finland converted state-owned bottling facilities to produce ~500,000 Molotov cocktails, which were integrated into their *"Motti"* tactics. Ukraine has followed a similar path by transforming commercial electronics and software expertise into a scalable drone ecosystem. In both cases, the decisive innovation was not the technology itself, but the ability to rapidly mobilize civilian industry to produce effective, low-cost weapons at-scale. The lesson for small states is rather than acquiring exquisite weapon systems, they should prioritize the creation of a framework and culture that fosters public-private collaboration.

Finally, Finland's Army Reserve system and organizations such as Lotta Svärd demonstrate how a prepared reserve force and societal mobilization reinforce denial and sustain resistance. Today, Baltic states' territorial defense organizations and Taiwan's All-Out Defense Mobilization Agency echo this integrated civil-military approach. Ultimately, the enduring lesson from the Winter War is that small states can deter stronger rivals through a strategy of denial, innovation, and societal mobilization.

Keywords: small state strategy, great powers, capability development, resilience, Winter War

TERESA DE ALMEIDA E SILVA*
DIOGO RIBEIRO CARDOSO[2]

SPACE AS A DOMAIN OF SMALL-STATE AGENCY: PORTUGAL, THE AZORES, AND STRATEGIC RELEVANCE IN GREAT POWER COMPETITION

*Institute of Social and Political Sciences (ISCSP-University of Lisboa) and Centre for Administration and Public Policies (CAPP), [2]Institute of Social and Political Sciences (ISCSP-University of Lisboa)

In an era of strategic competition, small states face mounting pressure to preserve agency within increasingly hierarchical security environments. This paper argues that outer space can function as a domain of strategic agency for small and medium powers, not through scale but through the logic of an emerging domain whose selected segments, particularly ground infrastructure, launch hosting, and return operations, combine relatively low entry costs with unusually high alliance externalities. Where a small state can fill a capability gap that larger allies value, investment converts into relevance disproportionate to material weight.

Portugal offers a revealing case. Traditionally seen as a peripheral actor, it has begun to reposition itself through a gradual expansion of its national space posture across diplomatic, military, and private dimensions: the consolidation of a space diplomacy agenda, the growing role of the Air Force, the transformation associated with Força Aérea 5.3, and the emergence of a national ecosystem with relevance for European and NATO resilience, innovation, and strategic autonomy. The Azores acquire renewed significance not only as a classic Atlantic geostrategic space, but as an emerging node in mitigating one of Europe's structural bottlenecks in access to and return from space, a domain where Europe still lacks mature capacity and where Santa Maria has moved to position itself early. Crucially, because this capability is nationally owned rather than ceded to an external power, its value to the alliance accrues on top of national autonomy rather than at its expense, reinforcing rather than constraining Portuguese agency.

Situating Portugal within the literature on small-state strategy, strategic domains, and great power competition, the analysis traces how geostrategic location, alliance embeddedness, and selective investment can convert into strategic relevance, with alliance utility as the dominant pathway alongside hedging leverage and strategic autonomy. It also considers the scope conditions under which this move is available to other small states. It concludes that small states gain strategic weight when they identify emerging domains in which geography, policy, innovation, and alliance utility can be combined into relevance that exceeds their traditional profile.

Keywords: small-state strategy, space as a strategic domain, Portugal, the Azores, European strategic autonomy

JEANETTE DE WEERT*

SOCIETAL RESILIENCE AGAINST COGNITIVE WARFARE

*The Netherlands Defence Academy

NATO member states are increasingly subject to cognitive warfare strategies that aim to divide societies and undermine trust in governments, democracy, Rule of Law, authorities, and science. This PhD project 'Societal resilience against cognitive warfare' intends to identify methods and interventions that aim to minimize the effectiveness of such hybrid threats to societal cohesion and stability. As part of this research, a scoping review of the literature on variables that potentially (co-)determine or predict cognitive warfare success is conducted.

National security is not only the domain of security forces but needs a whole-of-society approach. From a comprehensive security perspective, societal resilience is an essential aspect of protecting our nations, their democratic values, and our citizens against adversaries that try to erode our societal resilience for their own benefit. Democracies seem especially vulnerable to cognitive warfare methods due to their open structures and adherence to democratic values. Open structures and interconnectedness of European societies warrant a collaborative approach to combat cognitive warfare effectively. It asks for European strategic autonomy in the information environment.

So far, cognitive warfare is mainly viewed as a problem for security forces, intelligence agencies, or as a cyber/technological problem, rather than from the perspective of civil society. This, while civil society itself is one of its primary targets. This research brings the concepts of 'cognitive warfare' and 'societal resilience' together to be studied in relation to each other. This will lead to new academic insights and support policy decisions.

I would appreciate the opportunity to present (preliminary) findings and ideas at the conference and have a discussion with experts about the topic. This may provide new insights for all involved. Additionally, it would allow me to gather feedback from peers and improve my research.

Keywords: societal resilience, cognitive warfare, social cohesion, scoping review, hybrid

DARRELL DRIVER*

ARCTIC SECURITY REPORT: WHAT WE SHOULD WORRY ABOUT WHEN WE WORRY ABOUT THE ARCTIC

*Delphi Global Research Center

The US National Security Strategy, released in December 2025, contains around 10,000 words but none of them are “Arctic.” The strategy also omits references to similar words, such as polar or what NATO typically refers to as the High North. Nevertheless, it is increasingly difficult to engage with national security and defense professionals today when worries about threats and challenges emanating from the Arctic do not feature prominently. Melting ice, newly accessible sea lanes, and untapped resources are typically top of mind, especially in the evolving strategic competition with China. But are these the chief worries when one considers the security challenges the US and its allies are likely to encounter in the short to medium term? And, if not, does that mean the Arctic should not figure prominently in thinking about US and transatlantic security? The answers are “Not exactly” and “No.” The framing of the Arctic as an emerging theater of competition around thawing sea lanes is correct but incomplete. The Arctic is not a peripheral theater or NATO’s northern flank. It has been and remains the shortest path between nuclear powers and is home to the core of Russia’s second Strike Capability. It is, what one former advisor to President Trump called, “North America’s front door”. To be sure, it is a front door that is increasingly accessible: physically, economically, and militarily. If mismanaged, it could become an escalation accelerant in a broader crisis. Increasing accessibility only serves to exacerbate longstanding concerns that Cold War predecessors would have known well: nuclear stability, homeland defense, alliance management, and the long-term geometry of great power competition. The question is not whether the Arctic matters but how it matters and what exactly we should be worried about.

Keywords: Arctic, NATO, High North, Defense, security, Russia, China

AMBER FRENCH-GRIETTE*

THE CIVIC SHIELD: UNARMED RESISTANCE AS THE SECOND ARSENAL OF NATIONAL DEFENSE – LESSONS FROM UKRAINE FOR EUROPEAN HYBRID THREAT PREPAREDNESS

*Organization for Nonviolent Movements

Ukraine has resisted Russian aggression through two simultaneous arsenals: its armed forces, and what this paper terms its democracy arsenal, or civic shield – the aggregate of unarmed, citizen-driven actions that disrupt an aggressor's objectives and protect societal resilience. Drawing on 18 months of independent field research with military, ministry, and institutional actors across the United States, France, the Baltic states, and Ukraine, this paper examines unarmed civilian-based defense (UCBD) as a strategic complement to armed defense.

The paper documents how Ukraine's civic shield has manifested concretely: disabled veterans monitoring ceasefires, corruption-watchdog NGOs exposing supply chains behind Russian weapons systems, journalists and human rights lawyers documenting war crimes, citizens preserving cultural heritage under conditions of war, and so much more. Drawing on interviews with Ukrainian veterans, activists/volunteers, and institutional actors, including retired Colonel Andrii Ordynovych, the paper identifies a critical gap: Ukraine's civic resistance emerged largely through spontaneous volunteer energy rather than doctrinal integration. National Civil Resilience Strategy, a Law on National Resistance, and explicit roles for civil society networks in strategic defense planning were largely absent at the outset, leaving the civic shield without an adequate starting position.

The paper then turns to European preparedness, arguing that closing this gap requires two parallel tracks: an institutional track, in which civil society organizations engage defense ministries and armed forces on the latter's terms to integrate UCBD into national defense planning without subordinating it to military command; and a population-facing track, aimed at activating latent civic capacity across the broader population rather than hoping people will act under crisis. Engaging Schelling's bargaining-theoretic account of civilian resistance and contemporary evidence on nonviolent campaign effectiveness, the paper concludes by examining the deterrent value of civic preparedness itself, asking why authoritarian regimes invest so heavily in suppressing it.

Keywords: unarmed civilian-based defense, Ukraine, civic resilience, civil society

GÜVEN İÇÖZ*
FAHRI ERENEL[2]

BLUE CORRIDORS UNDER GREY-ZONE PRESSURE: OPERATIONAL LESSONS FOR MARITIME DEFENCE INNOVATION AND CRITICAL INFRASTRUCTURE RESILIENCE

*Global Savunma Magazine Research Center, [2]Istinye University

Maritime competition is increasingly expressed through limited pressure rather than open confrontation. Ports, offshore energy sites, subsea cables, commercial sea lines of communication, and strategic chokepoints can be exposed to coercion, disruption, and political signalling, while the threshold for declaring war remains untouched. This paper uses the concept of Blue Corridors to describe the maritime routes, chokepoints, and infrastructure networks through which trade, energy, military mobility, and strategic influence move.

The analysis focuses on the Black Sea and the Eastern Mediterranean. These two theatres show how grey-zone activity can affect defence planning through interference with shipping, pressure on ports and energy infrastructure, risks to subsea systems, unmanned systems, legal ambiguity, information pressure, and calibrated military signalling. Such activity may remain local in appearance, yet its consequences can extend to alliance coordination, deterrence, escalation control, and crisis management.

The paper draws on strategic-level security policy, defence diplomacy, NATO planning, and advisory experience. It develops three operational lessons for maritime defence innovation. First, the protection of Blue Corridors depends on interagency coordination, intelligence sharing, host-nation liaison, civil-military preparedness, and resilient infrastructure planning, in addition to naval presence. Second, grey-zone coercion requires decision-making processes that can integrate legal, political, military, and informational assessments amid uncertainty. Third, professional military education should use maritime grey-zone scenarios that connect infrastructure protection, strategic communication, crisis response and escalation management.

The study frames maritime defence innovation as an institutional challenge as well as a technological one. Platforms, sensors, and weapons remain central, but adaptation also depends on staff education, defence diplomacy, alliance procedures, lessons-learned systems, and resilience planning across contested maritime spaces. The proposed framework is intended to support military sciences in translating operational observation into practical defence adaptation.

Keywords: blue corridors, maritime defence innovation, grey-zone coercion, critical infrastructure resilience, strategic chokepoints

RUTH KAILA*

BUILDING MONETARY POWER THROUGH INFRASTRUCTURE: A NETWORK ANALYSIS OF CHINA'S DE-DOLLARISATION STRATEGY

*Finnish National Defence University

Contemporary great power competition extends beyond military capabilities to encompass broader forms of power exercised through critical infrastructures, financial networks, and strategic dependencies.

The international monetary system is characterised by a structural asymmetry: the United States operates from the centre of the global payment and reserve system, while other major economies must operate within the constraints created by this institutional and infrastructural configuration. In such a system, monetary power is exercised through control over network infrastructures and financial settlement chokepoints.

This article examines the internationalisation of the renminbi (RMB) as a process driven less by shifts in global currency preferences than by the construction of alternative financial infrastructures. Building on theories of monetary hierarchy and infrastructural power, the article develops a quarterly multiplex network dataset covering the period 2015-2025. The dataset integrates three dimensions of China's monetary architecture: bilateral central-bank swap-line capacity, connectivity within the Cross-Border Interbank Payment System (CIPS), and indicators of offshore RMB activity. From these layers, the study derives measures of infrastructural capacity, market-based de-dollarisation, and exposure to external payment chokepoints. By linking infrastructural development and market usage within a unified empirical framework, the analysis addresses a gap in existing research, which has typically examined macroeconomic determinants or individual institutional nodes separately.

The empirical results reveal a clear temporal pattern between infrastructure and market adoption. Expansions in swap-line capacity and CIPS connectivity systematically precede increases in market-based RMB usage and are associated with a gradual reduction in dependence on SWIFT-centred settlement channels.

More broadly, the findings highlight how states can pursue strategic objectives through the gradual construction of financial infrastructures that alter dependencies and reduce exposure to external coercion. In this sense, monetary infrastructures emerge as an increasingly important dimension of state power alongside more traditional military instruments.

Keywords: strategic autonomy, great power competition, economic statecraft, chokepoints, national power

SASU KATAJAMÄKI*

CHINA'S RECENT DUAL-USE POLAR AND DEEP-SEA SCIENTIFIC ACTIVITIES IN THE ARCTIC: CAUSE FOR CONCERN FOR THE NORDICS?

*Finnish National Defence University

Since its first Antarctic scientific expedition in 1984, China has conducted 42 Antarctic and 15 Arctic expeditions. These missions have formed a central part of China's polar science program and offer insights into the country's research priorities in the Arctic. During its most recent Arctic scientific expeditions, China has demonstrated rapid advances in developing technological means to access the polar depths. This presentation highlights China's recent polar scientific milestones and Arctic testing activities and discusses their relevance for the country's military-civil ambitions in the region.

In this regard, the tests of Jiaolong and Fendouzhe manned submersibles during China's 15th Arctic Scientific Expedition in 2025, alongside the country's efforts to test advanced polar deep-sea AUVs in the region, are presented as significant recent milestones. These tests, together with the country's other research priorities, demonstrate how China is seeking to build reliable means to navigate, communicate, and operate in the Arctic for both civil and military purposes. These means have been increasingly developed through applied dual-use polar research, which has been, in many instances, conducted by research institutions and universities with strong links to the People's Liberation Army (PLA), such as Harbin Engineering University.

The presentation overall demonstrates how China has increasingly, in recent years, sought to develop means to access the Arctic geography and particularly the under-ice and deep-sea domains. It also discusses the implications of these activities for the other Arctic states, particularly the Nordics, as well as China's potential strategic options in the region more widely. The research presented is related to the author's own PhD research on China's Arctic military ambitions and utilizes primarily Chinese-language sources.

Keywords: China, Arctic, dual-use, military ambitions, strategy

DAVID MANNING*
ROLAND HELLBERG[2]

WARTIME SUPPLY CHAINS AND GEOPOLITICAL DISRUPTIONS: VULNERABILITIES, MACROECONOMIC TRANSMISSION, AND STRATEGIC RESILIENCE

*Senior enlisted member, United States Air Force, Freelance Lecturer and Writer in International Relations, Military History, and International Defense Alliances, [2]Swedish Defence University

The paper examines wartime supply chains as complex systems shaped by the interaction of geopolitics, logistics, and macroeconomics. Modern supply chains, optimized for efficiency, cost reduction, and global integration, contain structural vulnerabilities that become highly visible during geopolitical conflict. Under wartime conditions, disruptions to production and transportation generate cascading effects across the global economy.

The paper identifies four key sources of fragility: 1) Dependence on geographic chokepoints, particularly strategic maritime corridors, concentrates risk and threatens global trade flows when disrupted; 2) Logistical overreach in extended or contested environments weakens the reliability and sustainability of military and economic operations; 3) The complexity of multi-tier supply networks reduces transparency and control, increasing the likelihood that localized disruptions escalate into systemic failures; and 4) Deep interdependencies between sectors such as energy, agriculture, and advanced manufacturing create nonlinear dynamics in which disturbances rapidly spread across industries.

Supply chain breakdowns generate inflationary pressures through shortages while simultaneously reducing economic output by interrupting production. These disruptions weaken labor markets through rising unemployment and declining demand, while increasing financial volatility and tightening credit conditions.

The paper proposes a resilience-oriented framework emphasizing diversification of supply sources, digital technologies for visibility and coordination, and the regionalization of supply networks. Supply chains must be reconceptualized as strategic infrastructure, requiring a shift from purely efficiency-driven models toward approaches prioritizing robustness, flexibility, and strategic foresight in an increasingly volatile global environment.

Keywords: wartime supply chains; geopolitical risk; supply chain resilience; strategic adaptation; macroeconomic disruption

JUHA MATTILA*

RECOGNITION OF COMPETITIVE FORCES IN CONTEMPORARY EUROPEAN MILITARY STRATEGIES

*Aalto University

The peaceful decades after the end of the Cold War are past. Contemporary European militaries are facing pressure to transform from multiple directions. For example, Russian expansionism, the rapid evolution of battlefield techniques showcased on the Ukrainian front, the improving performance of the Russian military-industrial complex, manpower shortages, rising prices for military platforms, and the disintegration of the global political structure are all creating pressure on European defence. How do the current European military strategies address these pressures?

This research aims to improve the understanding of the current military strategic posture and introduce additional frameworks for composing military strategy through the use of Porter's five competitive forces framework as a model for multidimensional strategic pressure. The competitive forces are transferred to military affairs, arming each dimension with contemporary threats or potential competition. The research analyses four European military strategies to examine how they address strategic pressure across all five dimensions simultaneously.

While the 2024 military strategies of Germany, Finland, Poland, and Sweden all recognise Russia as the most likely adversary, the analysis indicates that the other four dimensions are addressed differently. Most of the forces address the emerging threat posed by uncrewed platforms using a conventional approach. Only Germany recognises the logistics and sustainability challenge. All forces are adding numbers of troops and purchasing conventional platforms, but none of them recognises new entrants, i.e., hybrid or cognitive operations, or challenges in their customer, i.e., the population and infrastructure dimensions. Sampled strategies do not account for changes in substitutes, such as uncrewed swarming platforms.

Keywords: competitive forces, strategic analysis, military strategy, literature review

MATTHEW MCGLYNN*

THE FINANCIAL ARCHITECTURE BEHIND RUSSIAN SABOTAGE IN ESTONIA

*Consilium Advisory

Russian-attributed sabotage, such as arson, vandalism, and interference against NATO members, has generated a growing body of prosecutions across Europe and is now widely recognised as an expanding form of state-directed hybrid warfare. Existing analysis has concentrated primarily on attribution and on the profile of the recruited operator, while the financial layer linking handlers to operators remains comparatively underexamined.

This paper examines that layer through the financial networks and patterns evident in cases of Russia-linked sabotage in Estonia. Estonian courts and KAPO disclose more about the financing and conduct of these cases than is typical in comparable jurisdictions, and the national caseload is small enough to permit exhaustive coding. The analysis draws on public records and, where possible, interviews with relevant Estonian authorities.

It proceeds on three fronts. First, it reconstructs the financial flows behind the offences: the payment channels observed (cryptocurrency, over-the-counter cash, conventional banking, payment-in-kind), the sums involved and the activities they paid for, and the handler-operator patterns. Second, it assesses how anti-money-laundering (AML) and counter-threat-financing instruments have been applied in these cases, relative to the state-security statutes prosecutors more commonly invoke. Third, it identifies gaps in that toolkit where disruptive financial powers were available but unused, or unavailable altogether.

These findings are a starting point for wider comparison, not firm conclusions. They speak to the conference's theme of turning operational insight into defence innovation: the court files are the operational record, and reading them closely points to a concrete change in how the alliance responds. The paper shows where those financial tools are going unused, and where they could be extended or better joined up with the wider counter-sabotage effort both in Estonia and in other frontline NATO states facing the same campaign.

Keywords: sabotage, finance, hybrid war

LUKAS MILEVSKI*

WOULD IT WORK ON US? THE GOLDEN QUESTION ABOUT EFFECT IN MILITARY THEORY

*Leiden University

Many military and/or strategic theories have a simple but intellectually critical blind spot: would the proposed manner of military tactical/operational behavior also have such effects against us? Many military theorists and theories make promises about the consequences of military operations, and the promises which they make tend to be general in character: Douhet, Fuller, Liddell Hart, and other maneuver theorists. But if such attacks *are* general, then the question applies: would these operational methods, if practiced against *us*, have the same promised effects? Drawing partly on Western theories, the Chinese, too, are aiming for system paralysis and destruction, which suggests that they believe Western military and national security systems are vulnerable to such effects. They must imagine that they would work against us, too. Or, hypothetically, can Western mission command (assuming it exists) be paralyzed? Either answer (no/yes) is problematic for military theory and practice, but for different reasons. If the answer is no, then there is a fundamental intellectual problem at the heart of many military theories; readers and consumers of theory may be unprepared for contingency in practice and are being set up for potential strategic failure. If the answer is yes, then other questions are raised: is this effect *actually* a real inevitability, or do we just have specific vulnerabilities to that style of military behavior? If the latter, we return to contingency as we have to ask whether we can protect ourselves against it. This leads again to a short intellectual step: if *we* can, might not the enemy also? Modern military theory is generally insufficiently reflexive and too prone to making general claims without considering whether we would be equally vulnerable; such claims should be scrutinized more closely than they have been up until now.

Keywords: strategy, effects, theory, practice

TIARNACH MOONEY*

BEFORE THE WARNING: AMBIENT RESILIENCE BASELINE MONITORING AS A STRATEGIC INSTRUMENT AGAINST HYBRID THREAT EXPLOITATION

*BHA Advisors

Hybrid threat strategies succeed not by overwhelming resilient societies but by exploiting preexisting fragilities – eroded institutions, fractured social capital, legitimacy deficits – that make states vulnerable before any overt action begins. The strategic question is not detection or response. It is a baseline: do states and alliances know, continuously and in advance, where societal resilience is degrading?

This paper presents BEAR (Baseline Early-warning and Assessment of Resilience) as a case study in ambient resilience monitoring as a strategic instrument. BEAR tracks multi-domain indicators across political, social, institutional, security, and information environments, using cascade and tipping-point modelling to identify the threshold conditions under which hybrid operations gain traction.

The paper argues three propositions: 1) that most early warning architectures are reactive by design, systematically narrowing the decision window available to commanders and policymakers; 2) that the pre-conditions for successful hybrid operations are measurable and predictable with sufficient lead time for preventive action – but only if monitoring is ambient rather than event-driven; and 3) that closing the signal-to-decision gap requires better baseline intelligence, not better alerting systems.

Drawing on BEAR's application in fragile and conflict-affected environments and emerging European resilience contexts, the paper proposes a framework for integrating ambient baseline monitoring into NATO and national defence planning, and identifies the doctrinal adaptations required to make preventive resilience intelligence operationally useful.

Keywords: resilience, hybrid threats, grey zone activities

VLAD ONEȚIU*

AI-AUGMENTED CIVILIAN COUNTER-INTELLIGENCE IN CYBER-ENABLED FINANCIAL WARFARE

*CYBOV

Cyber-enabled financial fraud has evolved from isolated criminal activity into a sustained, industrialized assault on civilian populations. In Romania, organized fraud campaigns generate roughly 48,000 reported incidents annually, and that figure reflects only one in ten actual victims. The pattern is structural, not anecdotal: criminal and state-affiliated actors increasingly use financial fraud as a vector for cognitive disruption, erosion of trust in national institutions, and large-scale extraction of wealth from civilian populations. In hybrid threat terms, the citizen has become a frontline target.

The operational reality is asymmetric. Attackers coordinate at the scale of campaigns running identical fraud scripts across thousands of victims, rotating phone numbers, domains, and identities within hours. Institutional defenses, by contrast, react at the scale of individual identifiers, often days or weeks after the damage has been done. By the time a fraudulent number is validated and blocked, the campaign has already moved on. This is not a technological gap; it is a doctrinal one.

This research project proposes a bottom-up response to this gap. Rather than treating citizens as passive victims to be protected after the fact, the platform operationalizes them as a distributed civilian sensor network. Each fraud report submitted anonymously feeds an AI-driven analysis pipeline that recognizes not just the surface indicators (numbers, links, emails) but the underlying campaign pattern. When attackers change their tools, the system still detects the operation. Antimanipulation safeguards ensure that no single report or coordinated group of false reports can compromise the collective verdict.

In active beta since 2026, DEFENSIG is positioned not as a replacement for institutional defenses, but as the missing civilian layer in a collective national ecosystem where each defender sees only fragments of the same hybrid threat.

Keywords: frauds, financial warfare, artificial intelligence

ROLAND POPP*

PREDICTING A 'PHONY WAR'?: HOW THE UNITED STATES-IRAN MILITARY CONFRONTATION EVOLVED INTO A PROTRACTED CONFLICT

*Military Academy at ETH Zurich

For quite some time, a minority group amongst US strategists deliberating on possible scenarios and outcomes of a confrontation between the People's Republic of China and the US has framed the eventual progression of a military conflict as leading towards protracted war, as both sides would exercise restraint given the perceived dangers of miscalculation and nuclear escalation. My paper argues that analogous thinking should have been applied when estimating the contours of a potential military confrontation between Iran and the United States in the wider Persian Gulf region. Despite the missing, for now, nuclear dimension of such a conflict and the resulting absence of the 'entanglement dilemma' regarding conventional and nuclear C3I capabilities, the argument is that it was indeed foreseeable that a US-Iranian war would likely turn into an undecided and sluggish 'phoney war' – not all too different from the previous undeclared and increasingly costly confrontation between the two antagonists. Some analysts predicted that, after an initial intensive phase, both sides would exercise restraint given the disinterest of their regional allies in further escalation, the endangerment of civilian infrastructures and sea lines of communication of vital importance for the world economy, and the evolving military balance as a result of the proliferation of precision-strike systems to the Iranian side, the latter enabling Tehran to target the foundations of previous US military superiority. Looking at the internal debates within the US military and national security establishments, it was indeed clear that the most likely consequence of such a war would be economic warfare through naval blockades and counter-blockades, with intermittent military confrontations in the air and at sea. Such a protracted conflict would always be very difficult to end through a negotiated solution.

Keywords: US-Iran, Persian Gulf, Iran War, protracted conflict

STEPHEN SATKIEWICZ*

THE GRAND DESIGN OF META-STRATEGY: THE NEXUS OF WAR, ORDER, AND IDEAS

*Comparative Civilizations Review

This paper introduces the new concept of Meta-Strategy – the study of the nature and meaning of strategy as well as how different societies, cultures, and civilizations conceptualize war, peace, and world order. Going beyond traditional strategic studies, this concept investigates the deeper existential questions that underlie the strategic dimension across civilizations. This paper explores the deep historical, civilizational, and philosophical roots of these conceptual divergences, in what is termed the Military-Ideational nexus, as they relate to a rapidly evolving multipolar landscape. Such an ambitious endeavor will be achieved through a thorough metatheoretical synthesis drawing upon the insights of fields spanning Civilizational Sciences, Historical Sociology, International Relations, Complexity Sciences, and Strategic Studies. This paper also engages with the varied scholarship of Clausewitz, Colin S. Gray, Christopher Dawson, and Eric Voegelin. Meta-Strategy is not just a mere abstract theoretical construct, but ultimately helps serve to properly guide actual practical action. How we think about reality ultimately also guides how we act, and this is true for whole societies and civilizations. Meta-Strategy is the proper foundation for the study of Strategic History and Strategic Cultures.

Keywords: strategy, grand strategy, theory, geopolitics

DENNIS SULLIVAN*

THE EGGSHELL MATRYOSHKA: NESTED COHERENCE DECAY, NUCLEAR SIGNALING AS LIMBIC HIJACK, AND THE LIMITS OF WESTPHALIAN DETERRENCE

*The Astraea Initiative

Russian nesting dolls present an illusion of robustness – layer within layer, each appears solid, each protecting the next layer. The eggshell Matryoshka shares the structure with a difference: each layer is load-bearing, brittle, and its failure propagates inward. This paper argues that states are eggshell Matryoshkas: the mushroom cloud now standing as the last intact shell of one hollow inside. A validated Coherence Decay Function locates an Event Horizon at Ξ=0.35 below which civil conflict probability climbs from 4.6% to 36.1%. States nest coherence across three layers – governance, commercial, and social – each capable of independent failure. Contemporary nuclear strategy and conflict prevention share one foundational miscalibration: neither sees the layers. The cascade runs in two geometries. One direction is from outside-in: external shocks crack governance and propagate inward, as in Albania in 1997. The second direction is from inside-out: internal decay hollows the social substrate while exterior layers hold apparent integrity, until the False Binding Energy fails, and the outer shell implodes into the vacuum, as in Russia in 2022. Inside-out failure stays invisible until implosion. The mushroom cloud runs a limbic hijacking operation – existential dread suppressing Western policy options independent of actual probability. At Ξ=0.279, a state exhausts most strategic instruments. Nuclear signaling becomes the last threat reaching beyond its borders – the outer eggshell threatening catastrophe precisely because nothing remains inside. Where personal and state coherence decay functions converge, as they do when institutional buffers between sovereign and state collapse systematically – nuclear C2 reliability shifts from a function of institutional coherence to one of personal coherence; a variable Western strategic planning carries no framework to assess. The second geometry gives no warning. The outer shell falls inward into the vacuum it spent years concealing. Western strategy holds tools only for the first. The second ends eras.

Keywords: state coherence decay, cognitive warfare, limbic hijack, deterrence theory, prevention economics, Kantian Event Horizon

NINA-MARI TAYLOR*

THE IMPACT OF THE RUSSIA-UKRAINE CONFLICT ON FERTILISER DEPENDENCY AND FOOD SECURITY IN AFRICA

*Faculty of Military Science, Stellenbosch University

The 2022 Russian invasion on Ukraine lead to disruptions in the global food, fertiliser, and energy markets. This is due to Russia's dominant position in these global markets (Hosoe 2023). The Russia-Ukraine war resulted in the global food and energy markets immediately experiencing negative impacts with respect to food, fuel, and fertiliser prices (Nechifor et al. 2024). This impact does not only affect European or neighboring countries, it also has a negative influence on African countries characterized by relatively high commodity import reliance, as well as pre-existing fiscal and debt vulnerabilities (Raga et al. 2025). The implication is that African countries could experience greater negative economic and social impacts from the Russia-Ukraine war.

This study investigates the extent to which the Russia-Ukraine war has affected fertilizer availability and food security in African countries. The study will employ panel regression analysis using African data to analyze the impact of the Russia-Ukraine conflict on food security and fertilizer costs in Africa. The study will focus on African countries who are attributed with high dependence on imported fertilizers and food commodities. Emphasis will be placed on the Russia-Ukraine war and endeavor to provide an understanding of the impact of conflict on African countries and the vulnerabilities of developing countries to external conflict. The study intends to make recommendations pertaining to greater investment in African regional fertilizer production, agricultural diversification, as well as potential continental food system resilience to reduce Africa's exposure to future geopolitical shocks.

Keywords: food security, geopolitical conflict, panel regressions, Russia-Ukraine conflict

SANDRO TEIXEIRA MOITA*

AGE OF FAILED CAMPAIGNS: IS IT STILL POSSIBLE TO RECONCILE OPERATIONS WITH STRATEGY?

*Brazilian Army Command and General Staff School (ECEME)

The 21st century has seen numerous military campaigns undertaken by forces that, despite their great tactical proficiency, have been unable to translate tactical successes into strategic results. However, even with several cases, still, the use of force has been disseminated in current times as a possible solution to political impasses. Although there are already important academic and military reflections on such a phenomenon, its continuous manifestation is the cause of amazement, given the number of strategic failures seen. Seeking to understand the dynamics of this process, this presentation seeks to understand the key elements of this process, in which the Strategy is devoured by tactical and operational considerations, and in which no plan survives, even because there seem to be no plans. There is still another singular dynamic, occurring at this moment, which creates a perception of a "perfect storm": the paradoxical articulation of time in a campaign. Thanks to advanced AI and communications systems, the time of tactical actions has accelerated significantly, while in the operational and strategic dimension, the temporal movement has been inverse, in which a slowdown is perceived, with various considerations, ranging from enemies who understood the Western way of fighting, to logistical issues such as the production of ammunition and military material, among others.

Considering the crossroads of technological innovation, advanced weapons, creating a paradise of military fetishism for leadership, in addition to the temporal paradox, the question remains: Is there still a place for Strategy and strategic thinking in the 21st century?

Keywords: strategy, military operations, strategic thinking, strategic bridge

ANZELA TITOVA*

COGNITIVE WARFARE = NEUROLOGICAL MANIPULATION OF PERCEPTION IN THE DIGITAL AGE (CASE STUDY: RUSSIA'S STRATEGIC COMMUNICATION IN LATVIA DURING THE COVID-19 PANDEMIC)

*University of Florence

My master's thesis examines Cognitive Warfare as a theoretical framework for strategic communication targeting human perception, attitude formation, and decision-making, using Russia's strategic communication in Latvia before and during COVID-19 as a case study. Rapid technological development and an unregulated cyber dimension have created unprecedented conditions for spreading disinformation, challenging democratic societies. The thesis develops a theoretical framework examining critical thinking and perception formation through a neurocognitive psychology lens, drawing on neuroscience, cognitive psychology, and intelligence analysis to reconstruct the 'anatomy of perception'. The research then applies this theoretical framework to Latvia before and during COVID-19, since perception formation is shaped cumulatively over time. The case study uses discourse analysis of Russian-language and Latvian state communications, alongside survey data, vaccination statistics, electoral results, and policy documents, tracing how narratives on vaccine safety and state legitimacy align with mechanisms of influence (repetition, emotional framing, institutional distrust) and shifts in public attitudes. The analysis identifies patterns consistent with such influence: differential vaccine uptake, electoral shifts toward pro-Kremlin parties, and diverging institutional trust between linguistic communities. COVID-19 is treated not as a distinct phenomenon but as a crisis that made narrative influence visible: ordinarily, such influence stays hidden, but crisis conditions destabilize even long-stable protective narrative frames, deepening pre-existing divisions in social trust. Rather than establishing causation, the qualitative design reads these patterns as consistent with, not proof of, the hypothesized mechanisms, aligning with scholarship favoring qualitative-quantitative combination for robust attribution. The thesis identifies a tension in Latvia's resilience strategy: a unified, Latvian-language information space risks excluding those with a differently formed cognitive domain. It proposes cognitive domain inclusion extending resilience measures across linguistic communities alongside targeted media literacy and concludes that these measures, with further quantitative research, offer an evidence-based path to strengthening societal resilience as a whole.

Keywords: cognitive warfare, perception, cognitive psychology, strategic communication, Latvia

GRACE TOVKACH*

RETHINKING 'FROZEN' CONFLICT IN GEORGIA AND MOLDOVA: PROTRACTED EXHAUSTION STRATEGY AND IMPLICATIONS FOR WAR TERMINATION

*University of Tartu, University of Glasgow, and KIMEP University

The infamous frozen conflicts – Transnistria, Abkhazia, South Ossetia, and, formerly, the Donbas, Crimea, and Nagorno-Karabakh – are, in many ways, emblematic of peace and conflict in the post-Soviet space. Transnistria, Abkhazia, and South Ossetia are the three remaining frozen conflicts that have not presently escalated to "hot wars"; however, it is important to note that none of the post-Soviet frozen conflicts, when described as such, were or are truly "frozen", even in the absence of ongoing armed combat. Considering the extended nature of the conflicts, their precariousness, and their intentional destabilization by Russia, this paper argues that the remaining "frozen conflicts" in Moldova and Georgia constitute protracted wars of exhaustion between the state and Russia, with the latter using the de-facto entities as proxies.

This paper expands on Delbrück's theory of exhaustion strategy to consider exhaustion of not only the morale of enemy armed forces, but also of the general public and state support for the conflict. Beginning with the 1990-1992 Transnistrian War and the 1991-1994 wars in South Ossetia and Abkhazia, process tracing of hostilities in Moldova and Georgia from the 1990s to the present evaluates instances of exhaustion in hybrid and conventional warfare to determine the degree of reduction of both states' political and military will to reabsorb their separatist territories, and, in addition, analyzes potential trajectories for war termination.

This paper finds that Russia and the de facto entities have favorably manipulated a combination of attrition and exhaustion strategies for decades in Georgia, rendering a meaningful challenge of either adversary or persistent Russian influence highly unlikely, and implying either continued conflict or eventual Georgian defeat. While similar outcomes are observed for the Transnistrian question in Moldova, inconsistent Russian support has rendered exhaustion less effective and opened potential avenues for war termination through diplomatic reunification.

Keywords: frozen conflicts, exhaustion strategy, hybrid

MAKSIM VASSIN*

RUSSIA: FRIEND OR FOE? CONSTRUCTION OF THREAT PERCEPTION AMONG ETHNIC RUSSIANS IN ESTONIA

*University of Tartu

Studies conducted by the Estonian Ministry of Defence show that, even in 2026, 35% of ethnic Russians living in Estonia do not perceive Russia's expanding sphere of influence as a security threat, compared to only 5% of ethnic Estonians. The two ethnic communities may live side by side, but see vastly different sources of potential military threat, some even identifying NATO as a primary threat actor. Why do parts of the population reject enemy images constructed by political figures? Do different ethnic groups within the same country view threats similarly, particularly when the identity of one group is tied to the threat actor?

This study investigates how individuals from different ethnic backgrounds arrive at different threat judgments in the same geopolitical environment. Drawing on Rousseau's (2006) Construction of Threat Model, which views threat perception as a product of individual identity, state identity, and personal salient dimensions. Using public surveys conducted by the Estonian Ministry of Defence, together with qualitative interviews among residents of Estonia consisting of both ethnic Estonians and ethnic Russians from across the country, this paper shows how the perception of the Russian threat is formed among ethnic Russians in Estonia.

It finds a spectrum of threat perception, with Russia as a primary threat actor at one end and NATO on the other. The key factor determining where ethnic Russians position themselves along this spectrum is their level of integration into Estonian society, which serves as a proxy for their identity framework, collective memory narratives, and enemy images. The paper further identifies frequency of Russian media consumption, individual lived experiences, and economic hardship as other factors influencing the level of threat perception and identification with the Estonian in-group. These findings have significant implications for how states think about cognitive security within their borders, particularly where target audiences are highly fractured.

Keywords: threat perception, cognitive security, crisis communications, collective memory

ILZE VILKA*

SOCIETAL RESILIENCE AS A WILL TO RESIST: A MULTI-LEVEL FRAMEWORK FOR SMALL FRONTLINE DEMOCRACIES

*Rīga Stradiņš University, Social Sciences Research Centre

Societal resilience has become a central concept in contemporary security debates, yet its relationship with the will to resist remains insufficiently conceptualised. Existing approaches frequently focus on preparedness, crisis management, or post-crisis recovery, while paying less attention to the social mechanisms that enable sustained resistance under conditions of cognitive and hybrid pressure.

This paper develops a multi-level framework that conceptualises societal resilience as a will to resist. The framework integrates three interrelated dimensions, societal identity, cognitive resilience, and behavioural commitment, examined across individual, community, national, and international levels of analysis. Social capital, expressed through trust, norms, and networks, is treated as the enabling mechanism linking these dimensions, while cognitive warfare is conceptualised as a sustained stressor targeting societal cohesion and the conditions for collective action.

The framework is developed as part of an ongoing postdoctoral research project examining the nexus among economic development, social capital, and societal resilience in the Baltic States. Empirical work is currently underway through expert interviews and social network analysis, beginning with fieldwork in Latvia and Lithuania. The paper presents the conceptual framework and discusses its potential for analysing strategic fragility and the will to resist in small frontline democracies exposed to hybrid and cognitive threats.

The framework highlights how trust, social capital, and institutional legitimacy function as strategic resources that shape a society's capacity for collective action and resistance. The paper contributes to security studies and defence policy by offering a structured analytical approach that treats societal resilience as a strategic resource rather than solely a post-crisis outcome.

Funded by the Latvian Council of Science and the European Regional Development Fund, Postdoctoral Research project No. 1.1.1.9/LZP/1/24/136, 'The Nexus between Economic Development, Social Capital and Societal Resilience in the Baltic States'.

Keywords: societal resilience, will to resist, cognitive warfare, social capital, Baltic States

CHRISTINE WHITTAKER*

SYSTEMIC INTERDICTION: OPERATION STARVATION AND THE ENDURING LOGIC OF STRATEGIC DENIAL

*University of Wolverhampton

Operation Starvation demonstrated how strategic effect could be achieved through the disruption of interconnected maritime and logistical systems rather than through direct destruction alone.

This paper argues that the campaign exemplified a form of systemic interdiction in which aerial mining generated cascading economic and operational effects across Japan's wartime infrastructure. Situating Operation Starvation within broader debates surrounding denial theory and strategic bombing, the paper examines how interdiction of interconnected maritime logistical systems constrained Japanese strategic flexibility during the final stages of the Pacific War. Using Operation Starvation as a historical case study, the paper argues that the disruption of logistical networks generated strategic consequences extending beyond immediate physical destruction.

By connecting Operation Starvation's interdiction logic to contemporary A2/AD environments and maritime chokepoints such as the Strait of Hormuz, this paper demonstrates that modern denial strategies continue to exploit logistical vulnerability and dependence upon maritime chokepoints to generate disproportionate operational and economic effects.

While operational technologies have evolved substantially since 1945, the strategic logic of generating cascading effects through the disruption of critical logistical networks and maritime chokepoints remains highly relevant in contemporary denial environments.

Keywords: A2/AD, maritime interdiction, systemic Interdiction, strategic denial, chokepoint warfare

SHANG-SU WU*

CAMBODIA AND THAILAND: COMPARISON OF MILITARY MODERNIZATION

*Rabdan Academy

The armed conflicts on the border between Cambodia and Thailand in 2025 present an opportunity to compare two distinct ways of military modernisation. Cambodia has an internally oriented force structure that evolved from its civil war and has only a few sophisticated capabilities or advanced platforms. In comparison, Thailand has developed its armed forces with generally complete battle orders, mainly established during the Cold War. A lack of arms dynamics between Cambodia and Thailand was ended with armed conflicts in 2025. Their asymmetrical balance structurally influenced the 2025 battles, but it did not fully determine the course of the armed conflicts, given the limited nature of border conflicts. Afterwards, arms dynamics between these two Southeast Asian countries would be certain. New defense technologies, such as drones are introduced by both sides; however, conventional arms remain essential, and integration of the two categories of military capabilities would shape the bilateral balance of forces.

Keywords: Cambodia, Thailand, military modernisation

SHANG-SU WU*

LESSONS OF THE MIDDLE EAST WAR FOR TAIWAN

*Rabdan Academy

The US/Israel-Iran War is informative for the geostrategic dynamics in the Taiwan Strait, where the security outlook reflects China's motivation and capability to challenge the status quo, as well as responses by Taiwan and other related actors, such as the United States and Japan. The Middle East War, which has so far been conducted without land battle, demonstrates denial and control through three approaches: air strikes by the United States and Israel against Iran, Iran's denial of the Hormuz Strait, and firepower projection by Iran against regional countries, offering lessons about dynamics between control and denial in the Taiwan Strait.

Beijing has two sets of goals: Taiwan and related locations where interventions may be based, such as Japan and the Philippines. China can launch both air strikes and standoff firepower against Taiwan. Some Iranian measures, such as hardened construction and a decentralized command structure, may be learned by Taipei to ensure that certain capabilities are retained under attack. However, Iran's geographic conditions are different from those of Taiwan, namely size and location, which hampers a comparison. Beijing may threaten broader warfare to deter any third-party involvement or even pre-emptive strikes. But the war signifies limited impact from either air strikes or standoff firepower.

As for responses to Beijing's challenge, the lesson is that countervalue sea denial may be relevant, as seen by Tehran's use of limited naval capacity to create strategic leverage. Although no East Asian country is located at a critical chokepoint for China, adopting an economic approach would amplify the effect of sea denial. For example, a few symbolic attacks could dramatically increase China's shipping costs through rising insurance rates, a weakness of its export-driven economy.

Keywords: China, Taiwan, United States, denial, Japan

KONSTANTINOS XYPOLYTOS*

FROM DECISIVE BATTLE TO ENDURING FORCE: UTILITY, ACCESSIBILITY, AND THE PROLIFERATION OF WAR

*Bahcesehir University

Contemporary warfare remains tethered to an inherited expectation of decisiveness, the belief that force yields political resolution. However, this assumption increasingly misrepresents the modern utility of force. While shifts between centralisation and decentralisation are historically common, the current environment features a profound collapse in the barriers to organised violence. Cheap weaponry, ubiquitous communication, and systemic inequalities have democratised access to the means of initiating and sustaining war.

This expansion has not automated conflict; rather, technological saturation has multiplied human decision points and dispersed tactical agency. AI, drones, and networked systems have intensified the cognitive and political demands on fighters and societies. Modernisation narratives focused on efficiency often obscure the heightened role of human judgement in these decentralised battlefields.

Crucially, these dynamics affect more than just insurgents. Large states now wage wars defined by endurance and strategic indeterminacy, engaging in conflicts that freeze, resume, and recalibrate rather than conclude. Post-Cold War doctrines, premised on lean forces and managerial rationalisation, were designed for short, decisive wars. These have proven strategically fragile. Consequently, mass, industrial depth, and societal resilience have re-emerged as central variables, not as industrial relics, but as necessary responses to protracted conflict.

This shift represents a democratisation of war: the diffusion of tools, organisational capacity, and the political permissibility of violence. Under these conditions, force is less an instrument of decision and more a sustained societal test. When war is easily started but ended only with extreme difficulty, force ceases to decide and begins to endure. Recognising this transformation is essential for recalibrating strategy in an era of persistent competition.

Keywords: strategy, endurance, resilience

§