HARP
SANAT

WAR AND PEACE STUDIES CONGRESS (WAPSCON-2025) 21ST CENTURY ARMED CONFLICTS: CHANGING DYNAMICS AND EMERGING LESSONS (23-24 OCTOBER 2025-ONLINE) (BOOK OF PROCEEDINGS)

Editors:
(E) Tuğgeneral Prof. Dr. Oktay Bingöl
(E) Kur. Alb. Doç. Dr. Ali Bilgin Varlık
Dr. Öğr. Üyesi Selma Şekercioğlu Bozacıoğlu

HARP SANAT

Harp Sanat©
www.harpsanat.com
harpsanat@matbumedya.com
0850 304 22 03
Yayıncı Sertifika No 28740

Genel Müdür: Emrah Çelik
Genel Yayın Yönetmeni: (E) Tuğgeneral Prof. Dr. Oktay Bingöl
Editörler: (E) Kur. Alb., Doç. Dr. Ali Bilgin Varlık
Dr. Öğr. Üyesi Selma Şekercioğlu Bozacıoğlu
Yardımcı Editörler: (E) Kur. Alb., Cumhur Erentürk
(E) Alb.Dr. Hasan Yılmaz, Master Student, Talha Çağman
Son Okuma: Ali Bilgin Varlık
Mizanpaj : Yusuf Efe Civlez
Kapak Tasarım: Yusuf Efe Civlez

1. Basım, İstanbul, Temmuz 2026
ISBN: 978-625-5717-15-3
Tilki Kitap Matbaa / İstanbul
Matbaa Sertifika No: 48138

Harp Sanat Yayınevi tarafından baskıya hazırlanan eserlerin hukuki sorumluluğu tamamen yazara aittir.

WAR AND PEACE STUDIES CONGRESS (WAPSCON-2025) 21ST CENTURY ARMED CONFLICTS: CHANGING DYNAMICS AND EMERGING LESSONS (23-24 OCTOBER 2025-ONLINE) (BOOK OF PROCEEDINGS)

EDITORS:
(E) TUĞGENERAL PROF. DR. OKTAY BİNGÖL
(E) KUR. ALB. DOÇ. DR. ALİ BİLGİN VARLIK
DR. ÖĞR. ÜYESİ SELMA ŞEKERCİOĞLU BOZACIOĞLU

CONTENTS

HARP SANAT YAYINEVININ YAYIN ESASLARI

Harp Sanat Yayınevi, şanlı Silahlı Kuvvetlerimizde yıllarca görev yapmış olan emekli bir subay tarafından ülkemizdeki askeri tarih çalışmalarına katkı sağlamak için 2021 yılında kurulmuştur. Bilimin ışığını rehber edinen Yayınevimiz, Atatürkçü bir çizgide, bağımsız yayıncılık faaliyetlerinde bulunmayı temel ilke edinmiştir. Yayınevimiz, yayımlayacağı nitelikli eserlerle ülkemizde askeri tarih alanında hissedilen eksikliği gidermeyi amaçlamaktadır.

Bilindiği üzere toplumların tarihi incelendiğinde askerlikle ilgili hususların siyasi, sosyal ve kültürel alanlara doğrudan veya dolaylı etkilerinden söz edildiği görülmektedir. Bu etkilerin tespit ve değerlendirmesinin, günümüze ve hatta geleceğe bakan yönlerinin ortaya konulmasının fert ve devlet ölçeğindeki gelişime önemli katkılar sağlayacağı üzerinde durulmaktadır.

Sosyal bilimlerde askerî konulara ağırlık veren çalışmalar, Birinci Dünya Savaşı sonrasında önem kazanmaya başlamıştır. Zamanla genel tarih araştırmaları içinde kendine özgü bir anlayışa dönüşerek askerî tarih adı altında toplanan bu alandaki çalışmalar, Batı'da XXI. yüzyılda büyük bir hız kazanmışsa da Türkçe literatürde ne yazık ki henüz arzu edilen seviyeye ulaşamamıştır.

Karakter ve kültür kodlarımızda var olan askerliğe ve ona dair çalışmalara ivme kazandırılarak bu alandaki eksikliğin nitelikli eserlerle giderilmesine ihtiyaç duyulmaktadır. Aksi hâlde bu boşluğun akademik olmayan, ideolojik birtakım amaçlarla, bilgi ve belgeye dayanmayan yorumlarla ve popülist eserlerle doldurulması başka sorunları da beraberinde getirecek, ortak tarih bilincinin oluşumuna zarar verebilecektir.

Yayınevi olarak bu bilinçle, imkânlarımız nispetinde faydalı çalışmalar ortaya koymayı arzu ediyoruz. Bu alandaki akademisyen ve yazarlarla koordineli çalışmalar yürüterek akademik, tarafsız ve güvenilir kaynaklardan oluşan yerli ve yabancı nitelikli eserlerle okuru buluşturmak istiyoruz. Kuramsal kaynaklardan edebî eserlere kadar geniş bir yelpazede yapacağımız yayınlarla, askerliği

meslek olarak benimseyenlerin yanında askerî tarihe ilgi duyan herkese hitap eden akademik ve edebî eserler ile başvuru koleksiyonu oluşturmaya çaba sarf edeceğiz.

Tarihin tozlu raflarında unutulmaya yüz tutmuş, sandıklarda kilitli kalan hatıraların, yazma eserlerin, baskısı tükenmiş kitapların; Yükseköğretim kurumlarında büyük emekler verilerek hazırlandıktan sonra atıl kalan değerli çalışmaların gün yüzüne çıkarılması için atacağımız adımlarla, bu türdeki yayınların ve disiplinler arası müşterek akademik çalışmaların artmasında teşvik edici bir rol üstlenmek istiyoruz.

Askerlik mesleğinin ilgi sahası içinde önemli bir yer tutan yönetim, liderlik, strateji ve organizasyon konularıyla yeni modellere ilham verecek çalışmaları okurla buluşturmayı da hedefliyoruz.

Askerî geleneklerin oluşturulması, geliştirilmesi ve sürdürülmesi amacıyla özellikle tarihe mal olmuş komutan ve stratejistlerin düşünce ve tecrübelerinin sonraki nesillere aktarılmasına hizmet edecek biyografi ve hatıratlarının yanında tenkit ve kritiklerini yayınlamayı amaçlıyoruz.

Harp tarihinin konuları dışında kalan ancak yazarı veya işlediği konu itibariyle daha çok sosyal tarihin ve edebiyatın alanına giren eserlerin yayınlanmasının da önemli bir boşluğu dolduracağına inanıyoruz.

Her safhasını akademik bir titizlikle takip edeceğimiz, editörlük çalışmalarına önem vereceğimiz yayınlarımızda Türk Dil Kurumunun Yazım Kılavuzu'nda belirtilen esaslar çerçevesinde hareket edeceğiz.

Faydalı olabilmek niyet ve gayretiyle...

PREFACE

The nature of conflict in the 21st century is undergoing a profound and rapid change. As traditional military paradigms collide with burgeoning digital domains, the boundaries between war and peace, soldier and civilian, and physical and cognitive battlefields continue to blur.

The Second War and Peace Studies Congress (WAPSCON-2025) was held amid shifting global security dynamics and brought together military experts, policymakers, and academics to examine the emerging lessons of modern warfare. This congress has collected insights from 48 presentations across 12 specialized sessions, offering a comprehensive analysis of recent conflicts, from Ukraine to Gaza.

A central theme underscored throughout the Congress is that contemporary military effectiveness can no longer be measured solely by technological superiority or numerical mass. Instead, the modern battlefield demands adaptability, cognitive flexibility, and organizational learning. As highlighted by the participants, learning from these conflicts is not merely an academic exercise but a foundational step toward international peacebuilding. The findings detailed in briefings and the Congress's final report explore the convergence of traditional operations with new frontiers in cyberspace, space, and artificial intelligence. The findings address critical operational challenges, including the dilemma of drone-versus-drone warfare, the necessity of command center survivability in a transparent battlespace, and the logistical strain of high-intensity attrition. Furthermore, they emphasize the enduring importance of the human element—leadership, mission command, and the ethical responsibility to protect civilian lives amidst the automation of violence.

As we navigate an era of "subthreshold competition" and algorithmic complexity, the "technological treadmill" requires states to move beyond static bureaucracies. This book also provides actionable policy recommendations to foster "learning ecosystems" that link academia, the defense industry, and national planning. Ultimately, WAPSCON-2025 reaffirms that in the 21st century, victory—and the subsequent maintenance of a sustainable peace—will belong not only to those who innovate first, but to those who learn and adapt the fastest.

CONGRESS PROGRAMME

DAY-1 (23 OCTOBER 2025)

OPENING SESSION: JOINT WEBINAR – MICROSOFT TEAMS
23 OCT 2025 Thursday 10.00-11.30

Welcome Speech: Oktay BİNGÖL–(Rtd.) Brigadier General, Prof. Dr., Congress
Chairperson

Keynote Speech: (Rtd). General Ergin SAYGUN

Preliminary Presentations

WEBINAR-A

SESSION-1 (12.00-13.15): WAR AND POLITICS IN THE 21ST CENTURY

Moderator: Nazım ALTINTAŞ–(Rtd.) Lieutenant General

Presentations

Analysis of The Politics of Russo-Ukrainian War Through the Lens of Clausewitz
Talha Çağman–National Defense University, War Studies Master's Student/Türkiye

The Dimensional Changes of the Battlefields within the Historical Context
Cumhur Erentürk-(Rtd.) Colonel, Researcher/Türkiye

Harnessing the Power of Space in the Ukraine Conflict: Strategic and Operational Lessons
İnci Sökmen Alaca–Prof.Dr., Researcher/Türkiye

Geopolitical Lessons from Turkey's Strategic Success in Syria: Lessons for India's Défense and Security Policies
Faisal Banna M.–PhD Scholar, Pondicherry University/India

SESSION-2 (13.45-15.00): OPERATIONAL LESSONS IN THE 21ST CENTURY WARS

Moderator: Tahir BEKİROĞLU–(Rtd.) Lieutenant General, Dr.

Presentations

The Role of Airborne and Air Assault Operations in Modern Conflicts
Kosar Khazaei Poul–Master Student, Allameh Tabatabai University/Iran

How Does Hamas Benefit from its Web of Tunnels?
İbrahim Karataş–Assoc. Prof., Turkish Airlines

Where Science and Tactics Meet – A Comprehensive Guide to Improving Close Quarter Battle Training for German Conventional Police Units
Lea Bug–George C. Marshall Center for European Security Studies, Germany

The Dimensions of the Battlefields in Russia-Ukranian War
Cumhur Erentürk-(Rtd.) Colonel, Researcher/Türkiye

SESSION-3 (15.15-16.30): COMMAND-CONTROL-COMMUNICATION COMPUTER AND INTELLIGENCE

Moderator: Haldun SOLMAZTÜRK–(Rtd.) Brigadier General, Dr.

Presentations

New Command and Control System in Light of Multi-Domain Operations Concept: Battle NET
Eray Ekin–Exercise/War Gaming SME, CNK Global A.Ş.
Ahmet Berat İlhan –Military Information System SME, HAVELSAN

Command and Control Challenges in Multi-Domain Operations (MDO)

Suat Dönmez–(Rtd.) Brigadier General, Assoc. Prof, İstanbul Topkapı University/Türkiye

The Evolution of the Long Horizon Integrated Maritime Surveillance System-
Strategic Advance from the Homeland to the Blue Waters

Mesut Özel–(Rtd.) Rear Admiral, Assist. Prof., Kent University/Türkiye

AI-Driven Target Detection and Identification System for Military Combat Vehicles
Using Decision Support Matrix

Reşat Ali Tütüncüoğlu–Lead Trainer for C4ISR Systems, HAVELSAN
Selda Güney-Assoc. Prof., Başkent University

WEBINAR-B

SESSION-1 (12.00-14.45): 21. YÜZYIL SAVAŞLARINDA İSTİHBARAT VE MANEVRA

Oturum Başkanı: Hüsmen AKDENİZ–(E) Tümgeneral, Dr.

Sunumlar

İstihbarat Çalışmalarında Karşı İstihbarat ve Milli İstihbarat Teşkilatı'nın İKK
Faaliyetleri

Mustafa Tayfun Üstün–Doç. Dr., Atatürk Üniversitesi
Ömer Özger -Yüksek Lisans Öğrencisi, Atatürk Üniversitesi

Savaşlarda İstihbarat Faaliyetleri ve Alınan Önlemler Üzerine İnceleme

Mertkan Mert–Yüksek Lisans Öğrencisi, Kocaeli Üniversitesi

Geleceğin Savaşlarında Kuvvet Çarpanı Dronlar: Rusya-Ukrayna Savaşı Vakası

Mehmet Alkanalka–Dr. Öğr Üyesi, İstanbul Rumeli Üniversitesi

Hibrit Savaş/Hibrit Harekât Ortamında Muharebe Sahasının Tahayyülü ve Alınacak Dersler

Metin Sağsak–Dr.

İnsanlı ve İnsansız Takım (Manned–Unmanned Teaming–MUM-T) Konseptinin
Değişen Harekât Ortamındaki Rolü ve Gelecek Perspektifi

Hasan Çifci–Dr., HAVELSAN
Mehmet Altun–(E) Hv.Uçk.Bkm.Kur.Alb

Manevra Karma Sınıf Harekâtın Planlamasında Harekât Hızı

Levent Köse–(E) Tuğgeneral

Savaşın Geleceğine Bir Bakış ve Ukrayna-Rusya Savaşında Tank ve Zırhlı Araçlar Bakımından Alınan Dersler

Murat Kaymakçılar–(E) Albay, Savunma Havacılık ve Uzay Enstitüsü Derneği

Yapay Zekâ ve Caydırıcılık: Bir Senaryo

Özkan Kantemir–Dr., HAVELSAN
Altan Özkil–Dr., Atılım Üniversitesi

Günümüz Kentlerin Çatışma Alanlarına Dönüşmesi

Fatih Tümlü–Dr., Jandarma ve Sahil Güvenlik Akademisi

SESSION-2 (15.15-16.30): 21. YÜZYIL SAVAŞLARINDA DENİZ VE HAVA HAREKATIYLA İLGİLİ TESPİTLER

Oturum Başkanı: Nihat KÖKMEN–(E) Korgeneral

Sunumlar

Yeni Nesil Hava-Hava Angajmanları: Pakistan-Hindistan Örneği
Hüseyin Fazla–(E) Hv.Plt. Tuğgeneral, Dr., STRASAM Başkanı

Hava Harekâtında Kullanılan Elektronik Harp Teknik ve Taktik Uygulamaları: İsrail-İran 12 Gün Savaşı Örneği
Sargun Göktun–(E) Hv.Plt. Tuğgeneral

Balistik Füze Tehdidi ve Savunması Nedir? Entegre Hava-Füze-Balistik Füze Savunmasının Unsurları ve Gereklilikleri Nelerdir: İsrail-İran 12 Gün Savaşı Örneği
Hakan Kılıç–Savunma Analisti

Hava Harekâtında Kullanılan Modern Mühimmatlarda Son Yıllarda Kaydedilen Gelişmeler: Ukrayna-Rusya ve İsrail-İran Savaşları Örnekleri
Oğuz Ezik–(E) Albay

Deniz Harbinin Değişen Karakteri
Hakan Ercan–(E) Tuğamiral

Entegre Hava ve Füze Savunma Mimarisinde Hava Savunma Muhriplerinin Rolü
Mehmet Gürsu-Dr.
Ayhan Salar-Dr.

DAY-2: 24 OCTOBER 2025

WEBINAR-A

SESSION-4 (10.00-11.15): ARTIFICIAL INTELLIGENCE AND TECHNOLOGY IN THE 21ST CENTURY WARS

Moderator: Ali Bilgin VARLIK–(Rtd.) Colonel, Assoc. Prof.

Presentations

Redefining the Earth: GPS, GLONASS, GALILEO, BeiDou, and Fergani in Global Navigation Systems
Mahmut Can Özdemir–PhD Student, Yalova University

Evaluation of the Role of Artificial Intelligence in Shaping Peace in Regional Conflicts in West Asia
Parham Pourramezan–PhD, University of Tehran, Iran

Weaponization of Fake News: Battle of Narratives, War Medias, and Media Wars in the Case of 2025 Indo-Pakistani Tensions
Farzan Safari Sabet–PhD Student, University of Tehran
Maziar Mozaffari Falarti–Assist. Prof., University of Tehran

SESSION-5 (11.30-12.45): COMBAT SERVICE SUPPORT-LOGISTICS

Moderator: Alpaslan ERDOĞAN–(Rtd). Lieutenant General

Presentations

Logistics in Modern Warfare: Lessons from the Russia-Ukraine War
Bülent Durgun–Assoc. Prof., İstanbul Arel University

Logistics Lessons from 21st Century Wars: Sustainable Logistics: The Example of the Afghanistan War

Ahmet İlbaş–Assist. Prof., İstanbul Arel University

Hakan Kaya–Assist. Prof., İstanbul Arel University

Lessons from 21st-Century Wars with a Focus on Energy (Case Studies: Ukraine and the Second Nagorno-Karabakh War)

Rahmat Hajimineh–Assoc. Prof., Islamic Azad University, Tehran

Ebrahim Rezaei Rad–PhD Student, Azad University, Tehran

SESSION-6 (14.30-15.45): HUMAN SECURITY IN THE 21ST CENTURY WAR ZONES

Moderator: Selma ŞEKERCİOĞLU BOZACIOĞLU–Assist. Prof.

Presentations

Humanitarian Considerations in 21st-Century Warfare: Challenges and Solutions in the Era of Advanced Technologies and Asymmetric Conflicts

Samaneh Madhi–Master Student, University of Tehran

Women on the Frontlines: The Role of Female Soldiers in the Ukraine War

Deniz Kaynak–Research Assistant, İstanbul Arel University

WEBINAR-B

SESSION-3 (10.00-11.15): 21. YÜZYIL SAVAŞLARINDA SAVUNMA PLANLAMASI VE LOJİSTİK

Oturum Başkanı: Tarık ÖZKUT–(E) Tümgeneral, Dr.

Sunumlar

Asimetrik Savaş ve Askeri Lojistik: Rusya-Ukrayna Savaşı

Serkan Pasinlioğlu–Öğretim Görevlisi, Milli Savunma Üniversitesi

Rukiye Can Yalçın–Doç.Dr., Milli Savunma Üniversitesi

Savunma Kaynak Planlaması ve Stratejik Öngörü Arasındaki İlişki

Fahri Erenel–(E) Tuğgeneral Prof. Dr., İstinye Üniversitesi

Savunma Yönetiminin Konsept Gelişimi ve Gayrinizami Harp

Serkan Pasinlioğlu–Öğretim Görevlisi, Milli Savunma Üniversitesi

Ömer Faruk İşcan–Prof. Dr., Milli Savunma Üniversitesi

Tek Kanallı Yakın Kızılötesi Görüntülerden Transformer Tabanlı Monoküler Derinlik Tahmini

Gamze Nur Dağ–Endüstri Mühendisi, Eskişehir Osmangazi Üniversitesi

Elif Hakbilen–Endüstri Mühendisi, Eskişehir Osmangazi Üniversitesi

Sude Nisa Keskin–Endüstri Mühendisi, Eskişehir Osmangazi Üniversitesi

SESSION-4 (14.30-15.45): SAVAŞIN İNSANİ BOYUTLARI

Oturum Başkanı: Kemal DİNÇER–(E) Kurmay Albay

Sunumlar

Gazze Savaşında İki Tarafın Taktik ve Teknikleri

Ali Denizli–(E) Kurmay Albay, Prof. Dr., İstanbul Rumeli Üniversitesi

Muharebe Sahasında Günümüz Muharebe Özellikleri de Dikkate Alınarak Birliklerin Mühimmat İhtiyacı ve Karşılanması

Levent Köse–(E)Tuğgeneral

Savaşların Gizli Silâhı: Edebiyatın ve Sanatın Savaş Stratejilerine Etkisi

Gülten Akgül–Filolog, Millî Eğitim Bakanlığı

Kitle Kaynak Kullanımı ve Kitle Fonlaması ile Savaş Alanının Demokratikleşmesi:

Ukrayna-Rusya Savaşı Örneği

Cansu Ulu–Öğretim Görevlisi, Polis Akademisi Rüştü Ünsal Polis Meslek Okulu

21. Yüzyıl Çatışmalarında İnsancıl Hukukun Sınırları: Irak ve Suriye Örneği

Ayşe Miray Altay–Araştırma Görevlisi, Çanakkale 18 Mart Üniversitesi

21. Yüzyıl Savaşlarından Türetilmiş Etik ve Hukuk İçerikli Sonuçların Çözümlenmesi

Azize Serap Tunçer–Prof. Dr., Çankırı Karatekin Üniversitesi

Yapay Zekâ Destekli Karar Verme Süreçlerinin Askeri ve Sivil Alanda İş Sağlığı ve

Güvenliği Üzerine Etkileri

Vedat Caner–Dr. Öğr. Üyesi, İstanbul Beykent Üniversitesi

CLOSING: 24 October 16.30-17.00

JOINT WEBINAR

ORGANIZATION COMMITTEE

Oktay Bingöl, (Rtd.) Brigadier General, Prof., Merkez Strategy Institute/ Türkiye (Congress Chairperson)

Kemal Dinçer, (Rtd.) Colonel, Head of TESUD Bakırköy Branch/Türkiye

Ali Bilgin Varlık, (Rtd.) Colonel, Assoc. Prof. Merkez Strategy Institute/ Türkiye

Bülent Durgun, (Rtd.) Colonel, Assoc. Prof. İstanbul Arel University/Türkiye

Cumhur Erentürk, (Rtd.) Colonel, Tınaztepe Foundation/Türkiye

Selma Şekercioğlu Bozacıoğlu, Assist. Prof., İstanbul Arel University/Türkiye

Yunus Karaağaç, PhD., Researcher/Türkiye

Hasan Yılmaz, (Rtd.) Colonel, PhD., Researcher/Türkiye

Erol Işıkçı, (Rtd) Colonel, PhD., Researcher /Türkiye

Doğuş Sönmez, PhD., Research Assistant, Kadir Has University/Türkiye

Talha Çağman, Master Student, War Studies, National Defense University/ Türkiye

SCIENTIFIC ADVISORY COMMITTEE

Ahmet Ateş, Dr., Iğdır University, Intelligence and National Security Expert/Türkiye

Ahmet Berat İlhan, (Rtd.) Captain (N), HAVELSAN Researcher/Türkiye

Ahmet Yavuz, (Rtd.) Major General/Türkiye

Alaettin Sevim, (Rtd.) Rear Admiral /Türkiye

Ali Denizli, (Rtd.) Colonel, Prof., İstanbul Rumeli University/Türkiye

Ali Rıza Kuğu, (Rtd.) Brigadier, Dr., General/Türkiye

Alpaslan Erdoğan, (Rtd.) Lieutenant General/Türkiye

Alptekin Tartıcı, (Rtd.) Colonel, Dr., National Defense University Guest Lecturer/Türkiye

Anıl Çağlar Erkan, Dr., Energy Security and Public Diplomacy Expert/Türkiye

Arda Mevlütoğlu, Aerospace Engineer, Defense and Aviation Technologies, Procurement Programs and Industrial Policy Expert /Türkiye

Atakan Konukbay, (Rtd.) Colonel, Dr., HAVELSAN, CBRN Product Manager/Türkiye

Aytekin Cantekin, (Rtd.) Colonel, Dr., Military Academy Guest Lecturer/Türkiye

Başar Baysal, Assoc. Dr., Ankara Bilim University/Türkiye

Berkay Turgut, (Rtd.) Major General/Türkiye

Besfort Rrecaj, Assoc. Dr., University of Prishtina, Kosovo

Burak Semih Gülboy, Prof., İstanbul University, Politics and International Relations/Türkiye

Burak Şakir Şeker, (Rtd.) Captain, Assoc. Prof., Ankara Hacı Bayram Veli University/Türkiye

Can Kasapoğlu, Dr., EDAM Security and Defense Research Directorate/Türkiye

Celalettin Yavuz, (Rtd.) Colonel, Prof., World of Türkiye Author, Security Policy Expert/Türkiye

Cenk Özgen, Assoc. Prof., Giresun University, Defense Technologies Expert/Türkiye

Cengiz Tatar, (Rtd.) Colonel, Dr.

Chifu Iulian, Prof. Dr., National Defense University, Bucharest/Romania

Cihangir Akşit, (Rtd.) Major General, Dr., /Türkiye

Ceyhun Çiçekçi, Assist. Prof., Tekirdağ Namık Kemal University/Türkiye

Doğan Şafak Polat, (Rtd.) Colonel, Assoc. Prof., İstanbul Kent University/Türkiye

Ercan Caner, (Rtd.) Colonel/Türkiye

Efe Can Gürcan, Assoc.Prof., London School of Economics/UK

Emrah Özdemir, (Rtd.) Colonel, Assoc. Prof., Military Academy/Türkiye

Erdal Tatlı, (Rtd.) Colonel, Dr., Researcher/Türkiye

Ergin Saygun, (Rtd.) General/Türkiye

Ertan Beşe, Prof., Çankırı Karatekin University/Türkiye

Ethem Büyükışık, (Rtd.) Major General/Türkiye

Fahri Erenel, (Rtd.) Brigadier General, Prof., İstinye University/Türkiye

Fikret Birdişli, Prof., İnönü University/Türkiye

Gökhan Ak, (Rtd.) Colonel, Assist. Prof., İstanbul Topkapı University/Türkiye

Gökhan Koçer, Prof. Dr. Karadeniz Teknik Üniversitesi/Türkiye

Gökhan Sarı, (Rtd.) Colonel, Prof. /Türkiye

Hakan Eraydın, (Rtd.) Rear Admiral /Türkiye

Haldun Solmaztürk, (Rtd.) Brigadier General, Dr./Türkiye

Hasan Özyurt, (Rtd.) Rear Admiral, Defense Management Consultant, Unmanned Marine Vehicles Expert /Türkiye

Hüseyin Fazla, Dr., (Rtd.) Brigadier General, Strategic Researches Center Chairperson/Türkiye

Hüsmen Akdeniz, (Rtd.) Major General, Dr./Türkiye

Ivan Us, Chief Consultant, National Institute for Strategic Studies, Ukraine

Kaan Kutlu Ataç, Assist. Prof., Mersin University/Türkiye

Kadir Varoğlu, (Rtd.) Colonel, Prof., Başkent University/Türkiye

Kemal Eker, (Rtd.) Colonel, Dr., İstanbul Nişantaşı University/Türkiye

Leonid Polyakov, Advisor, National Institute for Strategic Studies/Ukraine

Levent Uzunçıbuk, (Rtd.) Colonel, Dr./Türkiye

Levent Köse, (Rtd.) Brigadier General/Türkiye

Lokman Ekinci, (Rtd.) Brigadier General/Türkiye

Mehmet Alkanalka, (Rtd.) Colonel, Dr./Türkiye

Mehmet Çanlı, (Rtd.) Colonel, Dr., Military Academy Guest Lecturer/Türkiye

Mehmet Daysal, (Rtd.) Major General/Türkiye

Mehmet Kınacı, (Rtd.) Colonel, NATO Allied Transformation Command/USA

Mehmet Kurum, Colonel, Dr., Gendarmerie and Coast Guard Academy/Türkiye

Mehmet Şahin, Assoc. Prof., Military Academy/Türkiye

Mesut Özel, (Rtd.) Rear Admiral, Assist. Prof., Kent University/Türkiye

Murat Ağdemir, (Rtd.) Colonel, Dr., Security and Terrorism Expert/Türkiye

Mustafa Şenol, (Rtd.) Brigadier General/Türkiye

Nazım Altıntaş, (Rtd.) Lieutenant General/Türkiye

Nihat Kökmen, (Rtd.) Lieutenant General/Türkiye

Nihayet Ünlü, (Rtd.) Brigadier General/Türkiye

Nuri Şen, (Rtd.) Colonel, Expert /Türkiye

Orhan Akbaş, (Rtd.) Lieutenant General/Türkiye

Öner Akgül, Assoc. Prof., National Defense University/Türkiye

Özgür Tüfekçi, Assoc. Prof., Karadeniz Teknik University International Relations/Türkiye

Özlem Kayhan Pusane, Prof., Işık University/Türkiye

Rafet Kılıç, (Rtd.) Major General/Türkiye

Rıza Bayrak, Assoc. Prof., Ostim Teknik University/Türkiye

Saffet Akkaya, (Rtd.) Colonel, Assist. Prof., Çağ University/Türkiye

Sait Karabayır, (Rtd) Colonel/Türkiye

Sait Yılmaz, (Rtd.) Colonel, Prof., İstanbul Esenyurt University/Türkiye

Savaş Biçer, (Rtd.) Colonel, Assoc. Prof., İstanbul Nişantaşı University/Türkiye

Serkan Yenal, Assoc. Dr., Military Academy /Türkiye

Suat Dönmez, (Rtd.) Brigadier General, Assoc. Prof., İstanbul Topkapı University/Türkiye

Şebnem Udum, Assoc. Prof., Hacettepe University/Türkiye

Tahir Bekiroğlu, (Rtd.) Lieutenant General, Dr./Türkiye

Tarık Özkut, (Rtd.) Major General, Assist. Prof., Okan University/Türkiye

Uğur Güngör, (Rtd.) Colonel, Prof., Başkent University/Türkiye

Ulaş Pehlivan, (Rtd.) Colonel, Peace Support and Security Expert, TERAM Author/Türkiye

Victor Korendovych, Prof., National Defense University of Ukraine

Yakup Battal (Rtd.) Brigadier General/Türkiye

CONGRESS CHAIRPERSON OPENING REMARKS

Dear Participants, Distinguished Guests, ladies, and gentlemen

It is my great honor and privilege to welcome you all to the International War and Peace Studies Congress 2025—organized under the theme "21st Century Armed Conflicts: Changing Dynamics and Emerging Lessons."

We gather here, across borders and disciplines, not only to study the anatomy of war but to understand how these experiences can serve as guideposts toward a more peaceful and secure world. The very essence of this congress lies in transforming knowledge born of conflict into wisdom for the sake of peace.

In an era when hybrid wars blur the boundaries between soldiers and civilians, and technology redefines not only the battlefield but also the moral dimensions of warfare, our collective responsibility is clear: to learn, to reflect, and to ensure that the lessons of war become the foundations of peace.

Now, I would like to provide you with an overview of the flow of the two-day program.

Our first day began with the Opening Session, featuring a welcome address and an insightful Keynote Speech by General (Retd.). Ergin Saygun, whose distinguished career and profound strategic vision will illuminate our congress theme. His reflections on the transformations in warfare will remind us that while the face of war may change, its human and ethical consequences remain enduring. Following the keynote speech, you will take three briefings on some critical dimensions of 21st-century wars, lessons learned, and actions taken.

After opening sessions, the congress divides into two parallel webinars—Webinar A and Webinar B—each exploring critical dimensions of 21st-century warfare.

In Webinar A, Session 1, titled "War and Politics in the 21st Century," scholars and experts will examine the intricate relationship between military strategy and political objectives. Presentations highlight that today's conflicts are as much about narratives and perceptions as they are about territory or force.

Session 2 will address operational lessons from 21st-century wars. From the strategic role of airborne operations to the tactical complexity of tunnel warfare and the integration of technology in close-quarters combat, this session bridges theory and practice.

Later, in Session 3, under the theme Command, Control, Communication, Computer, and Intelligence (C4I), speakers will focus on the transformative impact of artificial intelligence, integrated surveillance, and multi-domain operations. These discussions are vital in understanding how technological superiority and situational awareness shape both deterrence and defense.

In parallel, Webinar B will feature thought-provoking Turkish-language sessions. The first, "Intelligence and Maneuver in 21st Century Wars," examines counterintelligence, unmanned teaming, and the accelerating tempo of operations. The second, "Naval and Air Operations," focuses on lessons from the Israel-Iran conflict, the Indo-Pakistani engagements, and modern missile defense architectures.

Our second day begins with Session 4, "Artificial Intelligence and Technology in 21st Century Wars," which explores how cyber operations, AI systems, and unmanned technologies are reshaping both conflict and cooperation.

Session 5, focusing on Combat Service Support and Logistics, turns our attention to the backbone of every military campaign. The lessons drawn from Ukraine, Afghanistan, and Nagorno-Karabakh offer invaluable insights into sustainability, energy resilience, and strategic foresight.

In the afternoon, Session 6-"Human Security in the 21st Century War Zones-brings the discussion full circle, reminding us that beyond the machinery of war lies the human soul. Presentations on "Protection of Civilians in Gaza," "Women in War," and "Humanitarian Considerations in Asymmetric Conflicts" remind us that peace is not an abstract concept but a lived experience—fragile, essential, and deeply human.

Simultaneously, Webinar B continues with sessions on Defense Planning and Logistics and The Human Dimensions of War. Topics such as post-war urban reconstruction, ethical limits of humanitarian law, and the cultural reflections of warfare in literature and art bridge the analytical with the emotional, inviting us to view conflict not only through strategic but also through humanistic lenses.

Over the course of these two days, our congress will host distinguished participants, including generals/officers, professors, scholars, and young researchers, from several nations. This diversity is our strength. It reminds us that while wars may be fought within borders, peace must always be built across them.

Our discussions will no doubt be rich in military and technological insight. However, our ultimate mission is not to master the art of war, but to understand the necessity of peace. As Clausewitz famously observed, war is the continuation of politics by other means. But perhaps, in the 21st century, it is time for us to redefine that equation—to see peace as the continuation of war studies by wiser means.

As we embark on these two days of discussion, let us carry forward three guiding ideas:

Learning from Conflict: Every war, tragic as it may be, teaches valuable lessons about leadership, strategy, and resilience.

Integrating Technology and Ethics: The tools of war evolve, but our moral compass must remain steadfast.

Building a Culture of Peace: True security comes not only from deterrence alone, but also from understanding and cooperation.

I extend my sincere gratitude to the managers of the Turkish Retired Officers Association and the Rectorship of İstanbul Arel University, the distinguished members of our Scientific Advisory Committee, the Organizing Committee, the session moderators, the presenters, and all participants who made this event possible.

Thank you, and I wish you all an inspiring and fruitful congress.

(Rtd.) Brigadier General Prof. Dr. Oktay BİNGÖL
Congress Chairperson

(RTD) GENERAL ERGİN SAYGUN'S KEYNOTE SPEECH

Distinguished guests, colleagues, and dear participants,

It is a pleasure, if not a privilege, to address such a distinguished audience. My thanks go to the organizers and especially to Professor Oktay Bingöl.

The topic is most challenging, open to all sorts of discussion. But I promise to make it as painless as possible.

War is as old as humanity itself. Yet while its presence has endured through every era, its nature has changed beyond recognition. The weapons, the rules, even the boundaries of conflict are no longer what they once were. Today, we are witnessing not only new wars but a new logic of war — one defined by data, networks, and algorithms rather than trenches and frontlines.

There used to be a saying among staff officers: "Military history is a cadaver for us."

In earlier centuries, that "cadaver" — the record of past battles — was vital. It allowed officers to dissect what had happened, to learn how campaigns unfolded, and to prepare for future wars. But today, Warfare has transformed so completely that the past no longer provides reliable lessons for the future. The era of trench wars and cavalry charges cannot guide us through an age of cyber conflict, drones, and artificial intelligence.

The Evolution of Warfare

In its earliest forms, war was fought face-to-face — swords, shields, and sieges. Victory depended on courage, proximity, and terrain. The Industrial Revolution altered everything: factories enabled mass armies and mechanized destruction. World War I introduced chemical weapons, machine guns, and tanks. World War II brought radar, aircraft, and the nuclear bomb.

Korea saw the first jet aircraft. Vietnam became the era of the helicopter. The Gulf War demonstrated the use of precision-guided munitions and satellite-based targeting. Today, we are witnessing the age of unmanned systems and algorithmic warfare. It is The End of Predictable Conflicts For centuries, wars followed templates — ratios of attack to defense, fixed frontlines, clear hierarchies. That predictability has vanished.

Modern conflicts are fluid, decentralized, and multidomain. In Ukraine, we saw convoys operating under rigid centralized command suffer heavy losses against agile defenders with decentralized control. The lesson is clear: "An army built on centralized command and control cannot sustain initiative." Adaptability now outweighs mass; flexibility outperforms bureaucracy.

Unmanned Systems — The Drone Revolution

Perhaps no change is more visible than the rise of unmanned systems — in the air, at sea, and on land. Originally designed for reconnaissance, they now carry decisive, destructive firepower. In the Russia–Ukraine conflict, open-source intelligence indicates that Ukraine, although it has no navy, has damaged or destroyed roughly one-third of the Russian Black Sea Fleet, including the flagship Moskva. Drones and unmanned surface vessels have achieved what once required entire fleets.

These systems are small, inexpensive, and deadly — a $30 million Reaper UAV can be destroyed by 10-20 thousand drones. Similar tactics are seen in Yemen, where Houthi forces have struck naval and commercial targets, prompting the multinational Prosperity Guardian mission in the Red Sea.

Unmanned platforms' affordability and local manufacturability have democratized warfare, empowering even militias and terrorist organizations. Their limitations — range, payload, vulnerability to weather — are offset by rapid advances in autonomy and swarm coordination. The result is a new era of "mass precision" with no proportionality.

Cyber and Hybrid Warfare

The modern battlefield now extends into the digital realm. Although nothing new, Cyber operations can cripple a nation's economy without a single shot being fired. The 2021 Colonial Pipeline attack in the United States halted nearly half of the East Coast's fuel supply, proving that code can be as destructive as ordnance. Similarly, GPS spoofing and undersea cable sabotage in the Middle East and Baltic regions have disrupted navigation and communication networks.

Systems such as the U.S. Joint All-Domain Command and Control (JADC2) now seek to integrate land, air, sea, cyber, and space data into a unified decision network. Artificial intelligence analyses these inputs in real time, offering commanders multiple courses of action. No single force warfighting any longer. But with that speed comes a dilemma — as algorithms gain power, human oversight must not be lost.

Proxy Wars

Direct confrontation among major powers has become rare. Instead, influence is projected through proxy wars — smaller states or non-state actors fighting on behalf of global powers. Ukraine, Taiwan, Syria, and Yemen each illustrate this pattern. Proxy warfare minimizes political risk for sponsors but prolongs conflicts and blurs accountability. Even multinational banners — such as some operations claimed to be under NATO — may represent the agendas of a few individual nations.

Space — The New Battlefield

Outer space, once the domain of exploration, is now an extension of the battlefield. According to 2024 data from SIPRI and OECD, global space-defense spending exceeded $70 billion, led by the United States ($53 billion), China ($9 billion), and Russia (~$2 billion). Nations are deploying small satellite constellations for surveillance and communication, while developing anti-satellite weapons capable of disabling or de-orbiting rivals' satellites. The next major conflict may begin not in the skies, but beyond them.

Artificial Intelligence and Autonomous Warfare

Artificial intelligence is rapidly transforming command-and-control. AI enhances logistics, targeting, and threat analysis — compressing the decision cycle from minutes to seconds. Yet this very advantage introduces grave ethical and legal concerns. Who authorizes an autonomous strike? Who is accountable for error or collateral damage?

Delegating lethal decisions to algorithms challenges the principles of command-and-control responsibility and international humanitarian law. As one strategist observed: "We may soon win wars faster than we can justify them." Preserving human judgment is essential to maintaining moral legitimacy in warfare.

Economic Warfare and Sanctions

Economic warfare has become the most pervasive form of conflict. Sanctions, embargoes, and trade restrictions now serve as primary tools of coercion. According to 2024 IMF data, more than 12 000 active sanctions were in force worldwide — a record number. Sanctions must be declared by the UN. At present, only 14 sanctions fit this category. However, sanctions often yield unintended effects.

Türkiye, repeatedly subjected to arms embargoes, all by NATO Allies, has responded by developing a robust domestic defense industry — producing its own drones, tanks, and missile systems. Similarly, China, despite U.S. export restrictions, now holds over 55 percent of global patents in key emerging technologies, including nanotech and hypersonics.

As one Turkish leader said, "A bad neighbor makes one a homeowner; a bad ally makes one a manufacturer." Sanctions intended to weaken often end up catalyzing self-reliance and innovation.

The Future of Warfare

The next generation of warfare will be defined by human–machine collaboration and data-driven strategy. Future soldiers may command fleets of autonomous systems rather than lead battalions in person. Strategic advantage will depend on integration — combining technology, ethics, and adaptability. The main challenge lies not in building smarter machines, but in cultivating wiser humans — people who can balance speed with judgment and automation with accountability. Education, not armament, will determine who prevails in the wars of the future.

Conclusion

Ladies and gentlemen,

War today is no longer confined to the battlefield. It unfolds across economies, data networks, and societal perceptions. Victory will belong not to the strongest, but to the most adaptable — those who can combine knowledge with integrity, and power with restraint. As we enter an era of intelligent warfare, our duty is to ensure that intelligence remains guided by conscience. Technology should serve humanity, not define it.

If we forget that, the machines will not be needed to defeat us — we will have defeated ourselves. This much I think is enough before I challenge your patience.

I thank you once again for your kind attention.

May understanding, not conflict, be the enduring legacy of our time.

Thank you.

(Rtd). General Ergin SAYGUN

PART-1:

PRELIMINARY PRESENTATIONS SPECIAL BRIEFINGS

SPECIAL BRIEF-1

PRIMARY LESSONS LEARNED FROM 21. CENTURY WARS: ACTIONS OF SELECTED COUNTRIES

(Rtd.) Brigadier General, Prof. Dr. Oktay BİNGÖL

SPECIAL BRIEF-2

MILITARIZATION AND WEAPONIZATION OF SPACE:

A THREAT ASSESSMENT

(Rtd.) Colonel, Assoc. Prof. Ali Bilgin VARLIK

SPECIAL BRIEF-3

MODERN WARFARE LESSONS FROM UKRAINE AND GAZA:

DOTMLPFI IMPLICATIONS FOR FUTURE CONFLICTS

(Rtd.) Colonel, Dr. Hasan YILMAZ

PRIMARY LESSONS LEARNED FROM 21. CENTURY WARS: ACTIONS OF SELECTED COUNTRIES

Oktay BİNGÖL[1]

In this presentation, I will share some critical lessons learned from 21st-century wars. Before I start, I will briefly review the concept of Lessons Learned (LL).

LL is validated knowledge and experience derived from operations or exercises that improve effectiveness or efficiency when institutionalized in doctrine, training, or policy.

Cycle of LL includes:

1. Capture & Observation – Collect after-action reports (AARs), operational reports, and experiments,

2. Analyze – Identify causes, synthesize insights,

3. Validate & Decide – LL boards assign actions and deadlines,

4. Implement & Disseminate – Doctrine, training, and materiel updates,

5. Monitor & Close – Verify actual behavioral change.

It becomes "learned" only once corrective action has been successfully applied. Senior-level ownership is required to ensure that "lessons identified" (LIs) become "lessons learned" (LLs)—i.e., demonstrably embedded in practice.

There are seven main areas to be covered in this presentation. These are Drones & Counter-Unmanned Aerial Systems, EW/Electromagnetic Spectrum Operations (EMSO), Integrated Air & Missile Defense (IAMD), Munitions & Industry, Command-Control (C2)/Command-Post survivability, Urban operations, and Information Ops/Influence.

---

[1] Congress Chairperson (Rtd.) Brigadier General, Prof. Dr.

To explain each area, I will use a format that includes a description page and an action table. On the description page, you will see the title of the main area, and three parts: "What's changed", "Case study", and "Why it matters. There is a table on the action page that shows the actions taken by the United States, the United Kingdom, Ukraine, Russia, and China.

Drones & Counter-Unmanned Aerial Systems (C-UAS)

What's changed: Modern battlefields are saturated with unmanned systems—ranging from intelligence, surveillance, and reconnaissance (ISR) drones to loitering munitions, maritime USVs.

Case study — "Interdiction by First Person View (FPV), Pokrovsk axis (summer 2025)": Russian FPV swarms repeatedly struck vehicles along the T0515 MSR near Pokrovsk, forcing resupply by foot at night and stretching Ukrainian ground lines of communication. Analysts judged many injuries were FPV-caused, highlighting the need for both kinetic C-UAS and non-EW defenses when jamming is saturated or defeated.

Why it matters: Drones now achieve interdiction effects once reserved for aircraft, forcing adaptations in logistics, dispersion, and survivability on both sides in Ukraine.

Militaries are rapidly adapting by institutionalizing drone forces. Doctrines are shifting toward (1) mass, cheap, attritable UxS for ISR/strike; (2) layered counter-UAS (EW, guns, missiles, deception); and (3) distributed C2 so drone teams can survive in jammed airspace.

The goal: integrate counter-drone tools—from electronic warfare (EW) to kinetic interceptors—within each echelon, ensuring both proactive swarm deployment and reactive defense. Power projection now hinges on mastering drone swarms and neutralizing adversarial ones.

The actions taken by the states:

The United States DoD moved to layered C-UAS and massed autonomous systems (e.g., Replicator) across the force.

The UK MOD is building layered C-UAS across echelons. It is important to integrate, not buy stove-piped gadgets.

Ukraine created a new Unmanned Systems Forces and national drone programs to scale FPV/USVs.

Russia announced a dedicated drone branch to institutionalize battlefield UAS lessons.

China People's Liberation Army's analysts push stealthier, anti-jamming drones and swarming after watching Ukraine.

Electronic Warfare (EW)/ Electromagnetic Spectrum Operation (EMSO)

What's changed: Conflicts reveal that the electromagnetic spectrum (EMS) is a high-contest zone. The EM spectrum is a primary battlespace. Units plan for constant jamming/spoofing, strict signature discipline, and EM deception.

Case study — "Pokrova GNSS spoofing shield (2024-25)": Ukraine fielded a nationwide spoofing network ("Pokrova") to mislead Shahed-type OWA-UAVs and some PGMs, reportedly causing large fractions to miss or wander. Even partial success imposes massive cost asymmetry on the attacker and reduces interceptor expenditure.

Why it matters: Control of EMS determines whether drones, precision weapons, and C2 systems function at all—forcing armies to diversify their communications (fiber, hardline, line-of-sight relays) and accept degraded modes.

Doctrine now embeds EMS operations at the unit level—from tactical deception and jamming to resilient communications. Ukraine and Russia iterate fast (spoofing, direction-finding, counter-battery via emitter geolocate); the UK has long framed "information advantage," and the U.S. is embedding spectrum thinking across FM 3-0/ADP 3-13.

The actions taken by the states:

The U.S. training/doctrine system now assumes a highly contested EMS, emphasizing dispersion and signature control. The U.S. trains for dispersed, low-signature formations.

UK emphasizes whole-force EW integration.

Ukraine operates with a whole EMS-duel mindset.

Russia systematically scaled EW to blunt Ukrainian sensors/drones, sustaining theater-wide advantage.

China, by creating its Information Support Force, is reinforcing digital and EMS battle spaces as a primary domain.

Integrated Air & Missile Defense (IAMD)

What's changed: Salvo warfare mixes ballistic/cruise missiles with hun-

dreds of cheap drones—overwhelming point defenses unless sensors, shooters, and EW are fused across services and allies.

Case study — "Iran's April 13–14, 2024 mass strike on Israel": U.S. CENTCOM reported destroying 80+ one-way attack UAVs and multiple ballistic missiles in coalition IAMD operations—proof that integrated sensors, shared C2, and layered effectors can defeat very large salvos. Those lessons (allocation, cross-border cueing, partner integration) are informing allied doctrine and exercises.

Why it matters: Layered, coalition air defense—and smart shot allocation (save interceptors; use EW/kinetic guns vs. drones)—is now the difference between saturation failure and resilience.

Militaries are deploying multi-layered IAMD systems (e.g., Patriot, NASAMS, IRIS-T) supported by improved C2 and sensor fusion.

NATO and the U.S. are updating IAMD strategy/structures, while the UK's Land-GBAD aims to knit together different tools.

The actions taken by the states:

The U.S. DoD doubled down on coalition IAMD and kill-chains for large salvos after the April 2024 Iran strike.

The U.K. Army is launching Land-GBAD and a wider IAMD strategy focused on command-and-control integration.

Ukraine has built an IAMD web (Patriot/NASAMS/IRIS-T) and doctrine for defending cities/forces.

In Russia, doctrinal writing elevates counter-strike and air-defense integration after heavy attrition.

China Military Policy Review 2024 highlights the PLA's dense IADS and growing counter-salvo emphasis.

Munitions & Industry

What Changed: High-tempo, attritional combat demands industrial-scale resupply. The U.S. has invested billions in 155 mm lines and factories to achieve six-figure monthly output. Europe is scrambling to increase shell production to multi-million-dollar levels. NATO warns the alliance must rebuild industrial depth.

Case study — "U.S. artillery production surge (2024–26)": The Army opened new projectile-loading lines and green-lit a modern factory in Iowa.

Officials now project the 100k-per-month mark in 2026, not 2025—showing how hard scaling truly is and why planning assumptions must reflect industrial lead times.

Why it matters: Doctrine must assume "fight the factory": stockpiles, repair, and rapid reconstitution are as decisive as tactics.

The action taken by the states:

The U.S has prepared an industrial surge plan to 100k 155mm/month and new LAP lines—long-term contracts & capacity.

The UK invested heavily in continuous munitions supply and new facilities.

In Ukraine, domestic output (ammo/drone) expanded sharply with partner help.

Russian Strategy embraces attritional, industry-centric warfighting—mass stocks and sustainment.

China is accelerating missile and rocket production to sustain long-term high-tempo combat.

C2/Command-Post survivability

What's changed: Big, static HQs are artillery/drone magnets. High-precision targeting demands resilient, agile command post (CP) configurations.

Case study — "Ukrainian CP survivability TTPs (2024)": Ukrainian manual details camouflage/cover, EM discipline, route/tempo of displacement, and decoys to defeat RU ISR/fires—practical measures many NATO CPs still lack at scale.

Why it matters: Surviving to command is now a daily contest against persistent ISR. CP design is a warfighting function—not just a tents-and-trailers problem.

Forces are moving to small, mobile, dispersed CPs; tight EMCON; deception; and frequent displacement.

The action taken by the states:

The U.S. disseminates CP survivability TTPs from Ukraine.

In the U.K., post-Ukraine reforms emphasize resilient, distributed C2 and faster acquisition to field it.

Ukraine's CPs now fully incorporate movement, camouflage, and redundancy.

In the Russian armed forces, tactics evolved to protect C2 with dispersion, camouflage, and decoys under constant ISR.

China's reforms consolidate control functions within its Information Support Force, enabling tighter, faster, and more resilient battle management.

Urban Operations

What's changed: Warfare in built-up areas (Gaza City; Bakhmut/Avdiivka) presents unique challenges: civilian presence, infrastructure complexity, subterranean spaces, heavy C2 friction, and heavy ISR saturation.

Case study — "IDF in Gaza City (autumn 2023)": Reports summarize combined-arms in high-rise/tunnel terrain and the tradeoffs among tempo, fratricide risk, and collateral mitigation.

Why it matters: Urban campaigns now require drone-aware maneuvering (overhead threat), tunnel-clearing expertise, and more resilient comms—plus tighter fire discrimination under scrutiny.

Western armies are updating breaching, subterranean, counter-UAS over cities, fratricide prevention, and tempo control under legal/ethical constraints.

The action taken by the states:

The U.S. refines doctrine about tunnels, high civilian density, and decentralized tempo.

The UK leans into lessons drawn from Gaza and Ukraine to inform subterranean and dense urban fighting.

Ukraine's experiences in sieges like Bakhmut shape new breaching, route-clearance, and casualty-aware tempo.

Russia has adjusted assault formations and fire support for urban attrition.

China studies transparent urban battlefields to counter drone saturation and ensure command clarity.

Information Ops/Influence

What's changed: Information has become as lethal as a missile. Why it matters: Kinetic success can be undone by narrative failure; conversely, resilient, truthful comms can unlock aid, time, and legitimacy.

Case study — "Ukraine's StratCom during full-scale war": The Center for Strategic Communication and Information Security (SPRAVDI) coordinates messaging, counter-disinformation, and public guidance—illustrating how whole-of-government IO supports operational objectives and societal resilience in protracted conflict.

Militaries are embedding information advantage—narrative control, disinformation resilience, and strategic communications—into doctrine and operations.

The action taken by the states:

The U.S. builds "Information Advantage" into training and operations.

The UK integrates this across the MDI (Multi-Domain Integration) construct.

Ukraine's government actively counters disinformation via centralized comms. centers.

Russian doctrine now syncs IO with fires, cyber, and attrition.

China's Information Support Force places the information domain as a strategic axis of joint operations.

This concludes my briefing.

Thank you very much for your attention.

WAR AND PEACE STUDIES CONGRESS (WAPSCON)-2025

21ST CENTURY ARMED CONFLICTS: CHANGING DYNAMICS AND EMERGING LESSONS (23-24 OCTOBER 2025-ONLINE)

Primary Lessons Learned from 21. Century Wars & Actions of Selected Countries

Oktay BİNGÖL

References

- Military and Security Developments Involving the People's Republic of China . CNA Report, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF?
- MoD of Ukraine (Oct 29, 2024): Mass UAV procurement (1.8 million) with MoDigitalTransformation — scaling industrial capacity around drones. https://mod.gov.ua/en/news/for-2024-2025-the-ministry-of-defense-in-collaboration-with-the-ministry-of-digital-transformation-has-already-contracted-1-8-million-drones-totaling-nearly-uah-147-billion
- RAND (2025): "Implications of the Fighting in Ukraine for Future U.S. Military Operations", https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3100/RRA3141-2/RAND_RRA3141-2.pdf
- RUSI Occasional Paper: "Tactical Lessons from IDF Operations in Gaza (2023)", https://www.rusi.org/explore-our-research/publications/occasional-papers/tactical-lessons-israel-defense-forces-operations-gaza-2023
- RUSI commentary: "Closing the Say/Do Gap for UK Land Power", https://www.rusi.org/explore-our-research/publications/commentary/closing-saydo-gap-uk-land-power?
- RUSI paper: "Protecting the Force from Uncrewed Aerial Systems", https://static.rusi.org/protecting-the-force-from-uncrewed-uas.pdf
- RUSI: "Assuring the Tactical Sustainment of Land Forces", https://static.rusi.org/sustaining-land-forces-final-proof.pdf

References

- CALL memo: "Lessons Learned from the Ukrainian TDF: CP Survivability", https://api.army.mil/e2/c/downloads/2024/02/06/c1a5a9b6/24-862-tdf-cp-survivability-feb-24-public.pdf?
- CNA (2025): "Russian Concepts of Future Warfare Based on Lessons from the Ukraine War., https://www.cna.org/reports/2025/08/Russian-Concepts-of-Future-Warfare-Based-on-Lessons-from-the-Ukraine-War.pdf
- CNA (2023): "Learning Lessons from Ukraine: The Chinese PLA Is Watching.", https://www.rusi.org/explore-our-research/publications/commentary/russian-military-objectives-and-capacity-ukraine-through-2024?
- CSIS (2025): "Russia-Ukraine Drone War: Innovation on the Frontlines and Beyond.", https://www.csis.org/analysis/russia-ukraine-drone-war-innovation-frontlines-and-beyond?
- Jamestown China Brief (2025): PLA thinking about transparent battlefield & intelligentized warfare after Ukraine/Gaza. https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience?
- IISS Military Balance Blog (2025): "Combat losses and manpower… importance of mass in Ukraine." https://www.iiss.org/online-analysis/military-balance/2025/02/combat-losses-and-manpower-challenges-underscore-the-importance-of-mass-in-ukraine
- Military Review Space & Missile Defense special edition: Multiple articles on integrating Ukraine/Gaza lessons into U.S. IAMD and LSCO doctrine. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/March-2024/MR-Space-Missile-Defense-Special-Edition-UA1.pdf

References

- RUSI (2025): "Tactical Developments During the Third Year of the Russo–Ukrainian War", https://www.rusi.org/explore-our-research/publications/special-resources/tactical-developments-during-third-year-russo-ukrainian-war
- RUSI (2024): "Preliminary Lessons from Ukraine's Offensive Operations, 2022–23.", https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-ukraines-offensive-operations-2022-23
- RUSI (2024): "Tactical Lessons from IDF Operations in Gaza (2023).", https://www.rusi.org/explore-our-research/publications/occasional-papers/tactical-lessons-israel-defense-forces-operations-gaza-2023?
- RUSI (2023): "Stormbreak: Fighting Through Russian Defences in Ukraine's 2023 Offensive." https://static.rusi.org/Stormbreak-Special-Report-web-final_0.pdf
- RUSI commentary series: Russia's artillery war & innovation, https://www.rusi.org/explore-our-research/publications/commentary/russias-artillery-war-ukraine-challenges-and-innovations?utm_source=chatgpt.comU.S. Army
- TRADOC monograph: "How Russia Fights" https://api.army.mil/e2/c/downloads/2025/07/11/f2b1e75e/how-russia-fights-a-compendium-of-troika-observations-on-russia-s-special-military-operations.pdf?
- U.S. Army Infantry Magazine (Spring & Summer 2025): implementing small UAS & counter-UAS across "Infantry 2030" lines of effort. https://www.benning.army.mil/infantry/magazine/issues/2024/Spring/PDF/Spring24_InfMag.pdf?

Lessons Learned (LL)

Definition:

- Validated knowledge and experience derived from operations or exercises that lead to improved effectiveness or efficiency when institutionalized in doctrine, training, or policy.

Cycle:

1. **Capture & Observation –** Collect AARs, operational reports, experiments
2. **Analyze –** Identify causes, synthesize insights
3. **Validate & Decide –** LL boards assign actions and deadlines
4. **Implement & Disseminate –** Doctrine, training, and materiel updates
5. **Monitor & Close –** Verify actual behavioral change

It becomes "learned" only once corrective action has been successfully applied. Senior-level ownership is required to ensure that "lessons identified" (LIs) become "lessons learned" (LLs)—i.e., demonstrably embedded in practice.

Selected Lessons Learned

- **Drones & C-Unmanned Aerial Systems (C-UAS)**
- **Electronic Warfare (EW)/ Electromagnetic Spectrum Operations (EMSO)**
- **Integrated Air & Missile Defense (IAMD)**
- **Munitions & Industry**
- **Command and Control (C2)/Command-Post survivability**
- **Urban operations**
- **Information Operations/Influence**

……Topic……

- **What's changed:**
- **Case study:**
- **Why it matters:**

Actions by States

United States	United Kingdom	Ukraine	Russia	China

Drones & Counter-Unmanned Aerial Systems (C-UAS)

- **What's changed:** Modern battlefields are saturated with unmanned systems—ranging from intelligence, surveillance, and reconnaissance (ISR) drones to loitering munitions, maritime USVs.
- **Case study — "Interdiction by First Person View (FPV), Pokrovsk axis (summer 2025)"**: Russian FPV swarms repeatedly struck vehicles along the T0515 MSR near Pokrovsk, forcing resupply by foot at night and stretching Ukrainian ground lines of communication. Analysts judged many injuries were FPV-caused, highlighting the need for both kinetic C-UAS and non-EW defenses when jamming is saturated or defeated.
- **Why it matters:** Drones now achieve interdiction effects once reserved for aircraft, forcing adaptations in logistics, dispersion, and survivability on both sides in Ukraine.

Actions by States

United States	United Kingdom	Ukraine	Russia	China
DoD moved to layered C-UAS and massed autonomous systems (e.g., Replicator) across the force	MOD is building layered C-UAS across echelons. It is important to integrate, not buy stove-piped gadgets.	Created a new Unmanned Systems Forces and national drone programs to scale FPV/USVs.	Announced a dedicated drone branch to institutionalize battlefield UAS lessons.	PLA analysts push stealthier, anti-jamming drones and swarming after watching Ukraine.

EW/ Electromagnetic Spectrum Operation (EMSO)

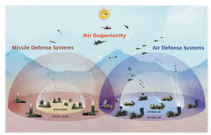
- **What's changed:** Conflicts reveal that electromagnetic spectrum (EMS) is a high-contest zone. The EM spectrum is a primary battlespace. Units plan for constant jamming/spoofing, strict signature discipline, and EM deception.
- **Case study** — "Pokrova GNSS spoofing shield (2024-25)": Ukraine fielded a nationwide spoofing network ("Pokrova") to mislead Shahed-type OWA-UAVs and some PGMs, reportedly causing large fractions to miss or wander. Even partial success imposes massive cost asymmetry on the attacker and reduces interceptor expenditure.
- **Why it matters:** Control of EMS determines whether drones, precision weapons, and C2 work at all—forcing armies to diversify comms (fiber, hardline, LOS relays) and accept degraded modes.

Actions by States

United States	United Kingdom	Ukraine	Russia	China
Training/doctrine now assumes a highly contested EMS, emphasizing dispersion and signature control. The U.S. trains for dispersed, low-signature formations.	UK emphasizes whole-force EW integration.	Ukraine operates with a whole EMS-duel mindset.	Systematically scaled EW to blunt Ukrainian sensors/drones; sustaining theater-wide advantage.	China, by creating its Information Support Force, is reinforcing digital and EMS battle spaces as a primary domain.

Integrated Air & Missile Defense (IAMD)

- **What's changed:** Salvo warfare mixes ballistic/cruise missiles with hundreds of cheap drones—overwhelming point defenses unless sensors, shooters, and EW are fused across services and allies.
- **Case study —** "Iran's April 13–14, 2024 mass strike on Israel": U.S. CENTCOM reported destroying 80+ one-way attack UAVs and multiple ballistic missiles in coalition IAMD operations—proof that integrated sensors, shared C2, and layered effectors can defeat very large salvos. Those lessons (allocation, cross-border cueing, partner integration) are informing allied doctrine and exercises.
- **Why it matters:** Layered, coalition air defense—and smart shot allocation (save interceptors; use EW/kinetic guns vs. drones)—is now the difference between saturation failure and resilience.



Munitions & Industry

- **What's changed:** High-tempo, attritional combat demands industrial-scale resupply. The U.S. has invested billions in 155 mm lines and factories to achieve six-figure monthly output. Europe is scrambling to increase shell production to multi-million-dollar levels. NATO warns the alliance must rebuild industrial depth.
- **Case study —** "U.S. artillery production surge (2024–26)": The Army opened new projectile-loading lines and green-lit a modern factory at Iowa; officials project the 100k-per-month mark in 2026, not 2025—showing how hard scaling truly is and why planning assumptions must reflect industrial lead times.
- **Why it matters:** Doctrine must assume "fight the factory": stockpiles, repair, and rapid reconstitution are as decisive as tactics.

Actions by States

United States	United Kingdom	Ukraine	Russia	China
Post–April 2024 Iran strike, DoD doubled-down on coalition IAMD and kill-chains for large salvos.	Army launching Land-GBAD and wider IAMD strategy focused on command-and-control integration.	Built an IAMD web (Patriot/NASAMS /IRIS-T etc.) and doctrine for defending cities/forces.	Doctrinal writing elevates counter-strike and air-defense integration after heavy attrition.	China Military Policy Review 2024 highlights the PLA's dense IADS and growing counter-salvo emphasis.

Actions by States

United States	United Kingdom	Ukraine	Russia	China
Industrial surge plan to 100k 155mm/month and new LAP lines—long-term contracts & capacity.	The UK invested heavily in continuous munitions supply and new facilities.	Domestic output (ammo/drone) expanded sharply with partner help.	Russian Strategy embraces attritional, industry-centric warfighting —mass stocks and sustainment.	China is accelerating missile and rocket production to sustain long-term high-tempo combat.

C2/Command-Post survivability

- **What's changed:** Big, static HQs are artillery/drone magnets. High-precision targeting demands resilient, agile command post (CP) configurations.
- **Case study** — "Ukrainian CP survivability TTPs (2024)": Ukrainian manual details camouflage/cover, EM discipline, route/tempo of displacement, and decoys to defeat RU ISR/fires—practical measures many NATO CPs still lack at scale.
- **Why it matters:** Surviving to command is now a daily contest against persistent ISR. CP design is a warfighting function—not just a tents-and-trailers problem.

Urban Operations

- **What's changed:** Warfare in built-up areas (Gaza City; Bakhmut/Avdiivka) presents unique challenges: civilian presence, infrastructure complexity, subterranean spaces, heavy C2 friction, and heavy ISR saturation.
- **Case study** — "IDF in Gaza City (autumn 2023)": Reports summarize combined-arms in high-rise/tunnel terrain and the tradeoffs among tempo, fratricide risk, and collateral mitigation.
- **Why it matters**: Urban campaigns now require drone-aware maneuver (overhead threat), tunnel-clearing expertise, and more resilient comms—plus tight fires discrimination under scrutiny.

Actions by States

United States	United Kingdom	Ukraine	Russia	China
The U.S. disseminates CP survivability TTPs from Ukraine.	Post-Ukraine reforms emphasize resilient, distributed C2 and faster acquisition to field it.	Ukraine's CPs now fully incorporate movement, camouflage, and redundancy.	Tactics evolved to protect C2 with dispersion, camouflage, and decoys under constant ISR.	China's reforms consolidate control functions within its Information Support Force, enabling tighter, faster, and more resilient battle management.

Actions by States

United States	United Kingdom	Ukraine	Russia	China
The U.S. refines doctrine about tunnels, high civilian density, and decentralized tempo.	The UK leans into lessons drawn from Gaza and Ukraine to inform subterranean and dense urban fighting.	Ukraine's experiences in sieges like Bakhmut shape new breaching, route-clearance, and casualty-aware tempo.	Russia has adjusted assault formations and fire support for urban attrition.	China studies transparent urban battlefields, countering drone saturation and ensuring command clarity.

Information Ops/Influence

- **What's changed:** Information has become as lethal as a missile.
- **Case study** — "Ukraine's StratCom during full-scale war": The Centre for Strategic Communication and Information Security (SPRAVDI) coordinates messaging, counter-disinfo and public guidance—illustrating how whole-of-government IO supports operational objectives and societal resilience in protracted conflict.
- **Why it matters:** Kinetic success can be undone by narrative failure; conversely, resilient, truthful comms can unlock aid, time, and legitimacy.

Actions by States

United States	United Kingdom	Ukraine	Russia	China
The U.S. builds "Information Advantage" into training and operations.	The UK integrates this across the MDI (Multi-Domain Integration) construct.	Ukraine's government actively counters disinformation via centralized comms. centers.	Russian doctrine now syncs IO with fires, cyber, and attrition.	China's Information Support Force places the information domain as a strategic axis of joint operations.

MILITARIZATION AND WEAPONIZATION OF SPACE: A THREAT ASSESSMENT

Ali Bilgin VARLIK[1]

Introduction

The militarization and weaponization of outer space denote the progressive integration of military capabilities and doctrines into the space domain by state and non-state actors. Militarization, in this context, extends beyond the deployment of satellites and technologies for strategic functions such as intelligence, surveillance, reconnaissance, communications, and global positioning. It also entails the adaptation of military doctrines, organizational structures, and operational concepts to accommodate space as a distinct warfighting environment. Consequently, outer space is increasingly recognized as an operational domain equivalent to land, sea, air, and cyber domains within contemporary military thought.

The weaponization of space, in turn, involves the development, deployment, and potential use of systems explicitly designed for offensive or defensive actions in, from, or through space. These include direct attack capabilities such as kinetic-energy and directed-energy weapons, as well as anti-satellite (ASAT) systems and associated enabling technologies.[2] While militarization primarily reflects the use of space for supporting terrestrial operations, weaponization signifies a more escalatory phase wherein space itself becomes a potential theater of conflict.

At present, satellites with military functions operated by 32 states are active in orbit. The United States, Russia, and China have incorporated space into their respective military strategies to a degree that ensures domain superiority. France, Israel, Italy, and India have also achieved significant ad-

[1] (Rtd) Col. Assoc. Prof., Merkez Strateji Enstitüsü, bilginvarlik@gmail.com, ORCID: 0000-0002-5265-2321

[2] James Clay Moltz. (2019). *The politics of space security: Strategic restraint and the pursuit of national interests.* Stanford: Stanford University Press.

vancements in integrating military-space capabilities, followed by a group of 25 other states possessing varying levels of satellite-based defense assets.[1] Reflecting this strategic evolution, NATO formally designated space as an operational domain in 2019, underscoring its growing centrality to collective defense and deterrence.[2]

When evaluated in light of contemporary geopolitical dynamics and rapid technological innovation, outer space emerges as a complex and multidimensional threat environment. Within this spectrum, the militarization of space represents an imminent strategic concern, while the weaponization of space embodies a more variable yet potentially destabilizing category of threats depending on the extent and nature of its implementation.

Methodology

The principal contribution of this study lies in establishing a comprehensive taxonomy of space-related threats, articulating the conceptual distinction between the militarization and weaponization of outer space, and conducting a threat assessment of both domains based on empirical data available up to and including the year 2024. This approach aims to contribute to the evolving discourse on space security by providing a structured analytical framework through which strategic risks and potential threats in the space environment can be systematically evaluated.

The research adopts a qualitative methodology as its primary analytical tool, supplemented by quantitative data analysis where the scope of inquiry necessitates numerical evaluation. Within this methodological framework, a comparative analysis is employed to assess the relative extent and nature of militarization and weaponization processes among state and institutional actors. This combination of qualitative and quantitative techniques ensures both interpretive depth and empirical rigor, allowing for a nuanced understanding of the dynamics shaping the contemporary space security environment.

The central research question guiding the study seeks to determine the degree to which risk, potential threat, threat, and danger have manifested in relation to the militarization and weaponization of space. In complement to

[1] Union of Concerned Scientists (UCS). (2023). UCS Satellite Database. https://www.ucs.org/resources/satellite-database, accessed 29.10.2025.

[2] NATO. (2020). *NATO's approach to space.* Brussels: NATO Public Diplomacy Division;

this main inquiry, subsidiary research questions address (a) the conceptual differentiation between space security and space safety, (b) the classification of counterspace technologies and weapons, and (c) the identification of distinct threat segments within the broader space environment.

The threat assessment, constituting the core analytical output of the article, evaluates the militarization and weaponization of space across five predefined threat categories. These categories are assessed using data synthesized from open-source materials, institutional reports, and relevant scholarly literature.

The study advances two primary hypotheses. The first pertains to the weaponization of space, positing that: "The current weaponization of space remains largely confined to dual-use technologies, counterspace capabilities, and ground-based systems designed to interfere with or disable satellites, rather than the stationing of offensive weapons in orbit." The second hypothesis concerns the militarization of space, arguing that the domain has undergone extensive militarization, reaching a level that can be categorized as a strategic danger within the spectrum of space-related threats.

Theoretical Framework

The concepts of militarization and weaponization of outer space are situated within the broader theoretical and policy framework of space security and safety. This overarching framework seeks to identify, categorize, and mitigate the spectrum of threats that may arise from or within the space environment. Conceptually, space security and safety encompass three principal threat dimensions:

Threats originating from space and directed toward Earth, such as the potential use of space-based assets for offensive operations or the re-entry of debris with destructive consequences; Threats to the ecological system of outer space, including the generation of orbital debris and environmental degradation resulting from human activity; and Threats to space systems, facilities, and operations, encompassing both intentional disruptions—such as cyberattacks, jamming, or anti-satellite operations—and unintentional hazards such as collisions or malfunctions.

These categories are not mutually exclusive; rather, they exhibit a high degree of interdependence and overlap, as a single threat may simultaneously affect multiple dimensions. The militarization and weaponization of space exemplify this overlap, as both processes extend across all three domains,

creating complex interactions between strategic, ecological, and operational risks.

To appropriately contextualize these two core concepts, the framework requires consideration of two analytical prerequisites. The first pertains to the conceptual scope of the term "threat", which must be defined in relation to the distinct characteristics of the space domain. The second concerns the placement of space-related threats within a broader threat taxonomy, enabling systematic classification and comparative analysis. Accordingly, before engaging directly with the main discussion, these two foundational elements are briefly outlined to provide the necessary conceptual grounding for the subsequent assessment of space militarization and weaponization.

The Concept of Threat

Within the field of security studies, the concept of threat is generally understood as a multidimensional construct composed of several interrelated elements that collectively determine its significance and magnitude. First, a threat presupposes the existence of a target or value, namely an entity, object, or principle identified as requiring protection. Such values may include sovereignty, territorial integrity, political stability, critical infrastructure, physical safety, environmental sustainability, survival, or social order. The identification of these referent objects forms the foundation upon which threat perception and subsequent policy responses are built.

Second, a threat entails a potential for harm, encompassing both direct and indirect dimensions. This harm may manifest as physical destruction or through structural, psychological, informational, economic, legal, or environmental impacts that compromise the stability or functionality of the targeted system. The severity of a threat thus depends not only on the nature of the harm but also on the vulnerability and resilience of the object under threat.

Third, every threat can be associated with an actor or source, whether state or non-state entities, technological systems, natural phenomena, or systemic crises. The identification of the actor or source is critical for determining intentionality, accountability, and the appropriate form of deterrence or defense.

Finally, threats inherently possess a temporal and uncertainty dimension. They are prospective in nature, characterized by variability in likelihood and intensity depending on contextual factors. For this reason, threat analysis is often conducted in tandem with risk assessment, which evaluates the probability and potential consequences of a given event.

To establish a coherent analytical framework for security assessment, it is essential to delineate the interrelated concepts of risk, potential threat, threat, and imminent danger. While these categories share conceptual similarities, they represent different stages along a continuum of escalation:

-Risk refers to conditions or developments that have not yet attained the characteristics of a potential threat. In such cases, the capacity, probability, or intent required for harm remain insufficient or absent.

-A potential threat denotes phenomena that exhibit the early indicators of a threat but have not yet materialized due to limitations in timing, capability, or intent.

-A threat exists when capacity, probability, and intent converge, even if actual harm has not yet occurred. It represents a situation with sufficient potential to cause damage under favorable conditions.

-Imminent danger arises when a threat reaches the stage of actualization, meaning that the harmful event is either occurring or explicitly impending. At this stage, the preconditions of a threat are fully realized, and immediate mitigation or defensive action becomes necessary.

This conceptual hierarchy allows for a systematic differentiation between varying degrees of peril and provides the analytical basis for assessing the evolving risks associated with the militarization and weaponization of space in subsequent sections of this study.

Threats within the Scope of Space Security and Safety

The concepts of space security and space safety constitute the foundational pillars of a peaceful, stable, and sustainable outer space environment. Both frameworks aim to ensure that the space domain remains a cooperative arena for scientific, commercial, and strategic activities, free from conflict and disruption. However, to effectively identify and assess threats to space systems and activities, it is essential to establish a shared conceptual understanding of these two closely related yet distinct terms.[1]

---

[1] Laetitia Zarkan. (2020). "What's in a word? Notions of "security" and "safety" in the space context", *UNIDIR*. https://unidir.org/commentary/whats-word-notions-security-and-safety-space-context, accessed 29.10.2025.

Although there is no universally accepted definition of space safety and space security, the United Nations General Assembly (UNGA) Working Paper A/AC.294/2022/WP.16, titled "Threats to the Security of Space Activities and Systems" (12 September 2022), provides a widely referenced distinction between the two concepts.[1]

Space safety generally refers to measures aimed at preventing accidental or unintentional harm to space systems, assets, or personnel. Such hazards may result from natural phenomena, including geomagnetic storms, micrometeoroid impacts, or radiation events, as well as anthropogenic causes, such as accidental collisions, design malfunctions, or operational failures. The primary objective of space safety initiatives is the mitigation of risk and the reduction of unintentional damage to space infrastructure. Within this framework, these occurrences are understood as risks rather than threats, as they lack intent or hostile motivation.[2]

In contrast, space security pertains to the protection of space systems and their components from deliberate interference or hostile actions by state or non-state actors. It encompasses preventive and defensive measures against intentional threats, such as jamming, cyber intrusions, anti-satellite (ASAT) operations, or the deployment of counterspace technologies. Moreover, space security extends beyond the technical protection of systems to include broader concerns related to international peace and strategic stability, including efforts by states and international organizations to prevent the weaponization and arms race in outer space.[3]

Although space safety and space security are often discussed in separate institutional contexts—typically within distinct working groups and legal frameworks of the United Nations—they are inherently interconnected. Certain issues, such as space debris, exemplify this overlap by posing both operational safety risks and strategic security challenges. Furthermore, linguistic and conceptual overlaps exist: in several languages, the terms safety and security are used interchangeably, reflecting the difficulty of separating the two dimensions in practice.[4]

1 United Nations General Assembly. (2022, September 12). *A/AC.294/2022/WP.16 Consideration of issues contained in paragraph 5 of General Assembly resolution A/RES/76/231: Threats to the security of space activities and systems.* Geneva.

2 Ibid., p. 2.

3 Ibid., p. 2.

4 Ibid., p. 2.

Ultimately, both safety and security are indispensable to ensuring the sustainability of space activities, defined as the long-term ability of all stakeholders to access, use, and benefit from outer space. Sustainable space governance requires maintaining an environment that is simultaneously safe from unintentional hazards and secure from deliberate threats, thereby enabling all actors to explore and utilize outer space "without discrimination of any kind, on a basis of equality and in accordance with international law".[1]

Threats within the Scope of Space Security and Safety

The taxonomy of threats to space security and safety reflects the multidimensional nature of the risks confronting both the space environment and its interaction with terrestrial systems. This taxonomy provides a conceptual structure for understanding how diverse phenomena—ranging from natural cosmic events to human-induced activities—can affect the stability, sustainability, and security of the space domain.

Table 1 below outlines the principal categories of threats within the scope of space security and safety, classified across three major domains: (1) threats from space to Earth, (2) threats to the space ecological system, and (3) threats to space facilities and activities. Each threat type is further evaluated according to its estimated severity—high, medium, or low—based on its potential for harm, likelihood of occurrence, and the degree of human control or mitigation available.

Table 1. Taxonomy of Threats to Space Security and Safety

	Threats from Space to Earth			**Threats to the Space Ecological System**			**Threats to Space Facilities and Activities**		
	High	Medium	Low	High	Medium	Low	High	Medium	Low
Threats from Space to Earth									
Asteroid and meteorite impact	X				X				X
Space weather and solar storms	X				X			X	
Supernova explosions	X				X			X	

1 Ibid., p. 2.

Extraterrestrial viruses	X				X				X
Space creatures	X					X		X	
Threats to the Space Ecological System									
Orbital debris (space junk)				X			X		
Biological contamination and back-contamination				X				X	
Light pollution and radio-frequency interference			X	X			X		
Overuse of geostationary and low Earth orbit capacity				X			X		
Effects of asteroid and planetary mining				X				X	
Chemical and particulate pollution				X				X	
Risks from solar power satellites and microwave radiation			X	X				X	
Threats to Space Facilities and Activities									
Natural cosmic threats			X	X			X		
Orbital traffic congestion and collision risks			X	X			X		
Weaponization and militarization of space	X				X		X		
Vulnerability of space-based economic systems		X				X	X		

Militarization of space: The militarization of space refers broadly to any military use of outer space, including non-weapon activities like military navigation systems [e.g., GNSS (Global Navigation Satellite System)] and organizational procedures and formations. Space has been militarized since the early days of exploration, and such use is not inherently aggressive or weapons-related.[1]

Weaponization of space: In contrast, weaponization involves the placement, deployment, or testing of weapons in space. Despite long-standing international discussions, there is no agreed definition of a "weapon" in space, leading many States to use the term counterspace technologies—referring to any capabilities designed to disrupt, damage, or destroy space systems, either reversibly or irreversibly.[2] The line between militarization and weaponization is often blurred. This is due to linguistic limitations in some languages and the lack of a universally accepted definition of "weapon".[3]

Types of Counterspace Technologies

Furthermore, counterspace capabilities are typically classified into four threat vectors according to their operational domain: (i) Earth-to-space, (ii) Space-to-space, (iii) Space-to-Earth, and (iv) Earth-to-Earth (UNGA, 2022: 2). Within this framework, Anti-Satellite (ASAT) weapons—often conflated with counterspace technologies—constitute a specific subset focused on targeting satellites. These systems can produce cascading debris effects, amplifying the risks to both military and civilian assets in orbit. The terminological confusion surrounding these categories reflects broader challenges in establishing comprehensive norms for the prevention of an arms race in outer space.

The typology of counterspace technologies, as identified by the United Nations General Assembly (UNGA), provides a comprehensive framework for understanding the diverse range of tools and methods that can threaten the stability and security of outer space. These technologies are generally categorized into kinetic (hard-kill) and non-kinetic (soft-kill) systems, each varying in destructiveness, detectability, and reversibility.[4]

Kinetic or hard-kill counterspace technologies are those that cause di-

1 Ibid., p. 2.
2 Ibid., p. 2.
3 Ibid., p. 2.
4 Ibid., p. 4-5.

rect physical destruction of a target. Among these, direct-ascent anti-satellite (ASAT) weapons are launched from Earth—whether from land, sea, or air platforms—to collide with satellites in orbit at extremely high speeds. A more sophisticated variant, the co-orbital ASAT, involves a system placed in orbit that maneuvers near its target using rendezvous and proximity operations (RPO). Such systems can execute multiple attack methods: direct collision, controlled explosions, or mechanical disruption through robotic arms. Some co-orbital systems can remain inactive for long durations, creating uncertainty about intent and purpose. Additionally, ground station attacks, which target terrestrial control centers that manage satellite communication and data relay, fall within the kinetic category. These attacks are typically irreversible, highly destructive, and relatively easy to attribute, but their most consequential byproduct is orbital debris, which can persist for decades depending on altitude.[1]

In contrast, non-kinetic or soft-kill counterspace technologies aim to disrupt or disable space systems without physically destroying them. Non-kinetic physical attacks, such as those employing lasers, high-powered microwaves (HPM), or electromagnetic pulses (EMP), can damage sensors or circuits instantaneously at the speed of light. Their effects range from temporary disruption to permanent damage, yet they are notoriously difficult to detect and attribute. Electronic (or electromagnetic) attacks, including jamming and spoofing, interfere with satellite communications by either blocking legitimate signals or injecting false ones. Although generally reversible, these methods can significantly impair the reliability of command, control, and navigation systems. Cyberattacks, targeting digital networks and data infrastructures, represent another critical threat vector. They can infiltrate satellites, ground stations, or user terminals to disrupt services, steal information, or manipulate functions. Despite their relatively low cost, cyberattacks can cause significant operational and strategic harm while remaining difficult to trace.[2]

Beyond direct attacks, the intentional creation of space debris is increasingly recognized as one of the most indiscriminate and enduring threats to all space activities. Unlike accidental debris, deliberate fragmentation events—often resulting from kinetic testing—generate long-lasting hazards. The European Space Agency estimates that more than 36,500 fragments exceed ten centimetres, one million range between one and ten centimetres, and 130 million measure between one millimetre and one centimetre, posing continuous collision risks.[1] Depending on orbital altitude, such debris can persist for decades or even centuries.

States have also identified harmful interference through electronic, cyber, or other non-kinetic means as a major challenge to maintaining operational stability in orbit. Furthermore, the proliferation of dual-use and dual-purpose objects—systems designed for civilian or scientific purposes but capable of serving military or intelligence functions—has amplified concerns about transparency and trust among spacefaring nations. This duality complicates verification processes and fuels strategic ambiguity, heightening the potential for misunderstanding and escalation in outer space.[2]

Types of Counterspace Weapons

The classification of counterspace weapons is closely linked to the types of counterspace technologies described previously, reflecting the methods, effects, and operational domains through which space systems can be targeted. Table 2 presents a structured overview of the principal weapon categories, their modes of operation, and their operational characteristics.[3]

1 Ibid., p. 4.
2 Ibid., p. 5.

1 European Space Agency. (2022, August 11). "Space debris by the numbers", https://www.esa.int/Space_Safety/Space_Debris/Space_debris_by_the_numbers, accessed 29.10.2025.
2 United Nations General Assembly. (2022, September 12). *A/AC.294/2022/WP.16, p. 6.*
3 Clayton Swope, Kari A. Bingen, Makena Young, & Kendra Lafave. (2025). *Space Threat Assessment 2025.* Washington: CSIS, https://www.csis.org/analysis/space-threat-assessment-2025, accessed 29.10.2025.

Table 2. Types of Counterspace Weapons

	Kinetic Weapons			Non-kinetic Weapons		Electronic Weapons		Cyber Operations
	Terrestrial Infrastructure Attack	Direct-Ascent ASAT	Orbital ASAT	Nuclear Detonations	Directed Energy	Jamming	Spoofing	
Origin to Destination	Ground-to-Ground	Ground-to-Space	Space-to-Space	Ground-to-Ground; Ground-to-Space; Space-to-Space	Ground-to-Ground; Ground-to-Space; Space-to-Space	Ground-to-Ground; Ground-to-Space; Space-to-Space	Ground-to-Ground; Ground-to-Space; Space-to-Space	N/A
Permanence of Attack	Permanent	Permanent	Permanent	Permanent	Varies, dependent on mode of attack	Not Permanent	Not Permanent	Varies, dependent on mode of attack
Scale of Attack Effects	Widespread, if node sup- ports multiple satellites	Widespread, if orbital debris creation	Limited to Widespread, dependent on mode of attack	Widespread	Limited and Regional, dependent on mode of attack	Limited and Regional, dependent on mode of attack	Limited and Regional, dependent on mode of attack	Limited to Widespread, dependent on mode of attack
Attributability of Attack	Variable attribution, depending on mode of attack	Launch site can be attributed	Can be attributed by tracking previously known orbit	Launch site can be attributed	Limited attribution	Modest attribution depending on mode of attack	Modest attribution depending on mode of attack	Limited or uncertain attribution
Requires Space Launch Capability	No	Yes	Yes	No	No	No	No	No
Requires Space Domain Aware- ness	No	Yes	Yes	No	Yes	No	No	No

This classification illustrates several critical aspects of counterspace operations:-Kinetic weapons, including terrestrial infrastructure attacks and ASAT systems, generally cause permanent and highly visible damage, particularly if they generate orbital debris. These attacks are relatively easier to attribute due to their physical signatures and known launch locations, and they often require space launch capability and domain awareness for successful execution.

-Non-kinetic weapons, such as directed-energy systems, can range from temporary disruptions to permanent damage depending on the mode of attack. While generally less visible than kinetic attacks, they may still produce significant operational impacts, including satellite sensor degradation or electronic incapacitation.

-Electronic weapons, including jamming and spoofing, primarily aim to disrupt communication and navigation signals. These attacks are often reversible but are difficult to trace to their source, increasing strategic ambiguity.

-Cyber operations target both terrestrial and space-based digital systems, potentially causing widespread disruption or corruption of satellite networks, ground control systems, and end-user terminals. The low cost and difficulty of attribution make cyber operations an increasingly attractive option for actors seeking strategic leverage without triggering kinetic escalation.

Overall, this typology highlights that the effects of counterspace weapons vary across multiple dimensions: permanence, scale, attribution, and technical requirements. Understanding these distinctions is essential for developing effective risk mitigation strategies, establishing norms of responsible behavior, and assessing the broader implications of space militarization and weaponization on international security.

Threat Segments of Space Security

The militarization and weaponization of space present multidimensional threats to the integrity and functionality of space systems. A comprehensive understanding of these threats requires an examination of the three primary components of space systems: ground installations, communication links, and space assets.[1] The ground segment encompasses fixed and mobile instal-

[1] Bruce Garino & James Gibson. (2009). "Space system threats", In Brian C. Tichenor (Ed.), *AU-18: Space primer* (pp. 273–282). Maxwell AFB, AL: Air University Press, p. 273.