Physical Education, Health and Social Sciences

https://journal-of-social-education.org

E-ISSN: 2958-5996
P-ISSN: 2958-5988

Hybrid Warfare and Criminal Networks

Faraz Amin Khan[1]

[1] MSc Criminology, Gomal University Dera Ismail Khan, Khyber Paktunkhwa, Pakistan,
Corresponding Authour's Email: 45faraz12@gmail.com

DOI: https://doi.org/10.63163/jpehss.v4i1.1630

Abstract

The current international security situation is characterized by the convergence of hybrid warfare and transnational criminal networks, creating multi-faceted challenges and issues for states, international organizations and law enforcement. Hybrid warfare is a mix of regular military forces, non-traditional warfare, cyber operations, information control, economic coercion and political manipulation for purposes below the threshold of open warfare. Meanwhile, criminal groups have also branched out into cybercrime, narcotics, arms smuggling, money laundering, human trafficking and sanctions evasion, establishing durable transnational networks, and all the while, they are increasingly drawn to the lucrative profits in the private sector. Today such networks serve as force multipliers in the operations of hybrid warfare, offering technological know-how, illicit funding, and cross-jurisdictional versatility. The estimated cost of cybercrime is approaching US$10 trillion per year, globally, and the estimated cost of money laundering 2–5% of the world's GDP. This paper analyzes the strategic embedding of criminal networks in hybrid operations, identifies new threats and looks at policy options for curbing criminal networks without compromising international security, rule of law or financial stability.

Keywords: Hybrid Warfare, Transnational Criminal Networks, Cybercrime, Money Laundering, Illicit Financial Flows, Geopolitical Security, Ransomware, Arms Trafficking, Human Trafficking.

Introduction

International security and warfare is dramatically changing in the twenty first century. While traditional conflict involving conventional military forces continues, it is also being supplemented, or in some cases redefined, by hybrid warfare strategies that combine the use of conventional military forces with irregular tactics, cyber, disinformation, economic, political influence and organized criminal networks. Hybrid warfare helps state and non-state actors to achieve goals without going to war, to cut down political risks and to obfuscate responsibility (Osman, 2026). Security doctrines must be flexible enough to accommodate the deliberate mix of military and non-military instruments, as it undermines traditional notions of defense and sovereignty. Hybrid warfare is the nexus between peace and open war, it is attacking in the middle, taking advantage of the weaknesses in cyberspace, financial system, governance and social system. Hybrid actors can achieve their aims and degrade opponents through asymmetric tactics, such as stoking the violence of proxy groups or influencing the actions of governments through covert operations. Some of these operations routinely consist of manipulation of information, psychological operations, the use of proxy actors, and cyberattacks against critical infrastructure which make legal and strategic counter-actions under international law complex (Ding, 2026).

This unpredictability in the situation makes it difficult to attribute events and to act on them because of the political, legal and operational limitations, which makes it difficult to preserve legitimacy while minimising security risks.At the same time, TOC has become a mature and

worldwide interdependent organized model of crime. Today's criminal organizations transcend national boundaries and pursue a variety of illegal activities such as drug and arms trafficking, human smuggling, cybercrime, environmental crimes, illicit financial flows and sanctions violations. These networks have developed advanced technological and financial networks, flexibility of operations which can be used to good effect in the context of poor governance, corruption and conflicts for monetary gains (Mehmood, 2026). Incorporation of organized crime into a hybrid warfare scenario gives an extra leverage for the strategies to operate by force multipliers using criminal networks for state sponsored or proxy operations. Hybrid warfare and criminal networks have become hallmarks of today's security threats. Criminal organisations are now often being hired to carry out cyberattacks, providing funding and weapons, providing intelligence and contributing to destabilising political leaders. This symbiotic relationship helps the operational reach and deniability of hybrid campaigns, thus allowing actors to conduct campaigns to achieve their objectives while lessening the risk of being held accountable. Conversely, criminal organisations also benefit from state protection, increased markets and opportunities created by the conflict, thereby establishing mutually reinforcing dynamics between strategic and illicit actors (Stavropoulou, 2026).

Recent wars are examples of how this convergence is being put into practice. In Russia–Ukraine war, cybercrime groups have been involved in ransomware, malware, and influence operations, all in service of geopolitical goals. The creation of advanced luxury trade laundering and sophisticated financial networks, such as shell companies, cryptocurrency exchanges and other circumvention smuggling operations, are being encouraged as a viable means of financing through economic sanctions placed by targeted states. Drug cartels in Latin America are increasingly using military-grade technology, encrypted communication systems, and cyber, and the line between the two groups organised crime and insurgent groups – is becoming more indistinct. In Africa and the Middle East, armed groups depend on criminality in the form of unlicensed trade in minerals, oil, drugs, and weapons, and they also form links with internationally active transnational criminal organizations (TCOs) (Zandieh, 2026). These hybrid threats have been enabled by technological innovation. Cryptocurrencies, encrypted messaging, artificial intelligence, commercial satellite imagery, unmanned aerial systems and dark web marketplaces lower the barrier to entry for criminal groups and enhance the sophistication of the operation. Today, critical infrastructure, financial organizations, healthcare systems and government-based networks can be attacked anywhere in the world with a few clicks and for managing costs, for which criminal networks are already playing a strategic role in so-called hybrid attacks. At the same time, those technologies create much concern for law enforcement organisations, as they need to 'catch up' with multipliers. Criminal networks that practice hybrid operations have been further strengthened by financial globalization. Illicit financial flows result from transnational crimes are estimated to cost hundreds of billions of dollars a year and rival the resources of national governments. Criminal organisations can leverage public institutions using these resources to gain access to superior technology, specific people and to operate for prolonged periods. The ability to funnel criminal proceeds through financial services allows for increased security of operations and further the value of the payment systems to state or proxy hybrid actors (Maritan, 2026). The collision between hybrid warfare and transnational crime has implications beyond the traditional views of national security. Hybrid threats by a well-organised corporate criminal network threaten democratic governance, undermine economic security, erode public confidence, compromise supply chains, threaten critical infrastructure and the enforcement of international law. Elections can be influenced by the use of similar disinformation, which is paid for with illegal profits. Attacks on the energy/transportation systems can drive economic disruption, and smuggling and trafficking networks enable the spread of weaponry, terrorism, and irregular migration. There is an increasing level of international acceptance of this phenomenon as strategic challenge. The recognition of

governments regarding organised crime—no longer as a problem of law enforcement but as a security matter related to the national defence. Intelligence agencies, military planners, cybersecurity authorities and financial regulators have been reintroducing increased coordination and cooperation in order to address threats that go beyond the traditional inter-agency boundaries. Today, legal enforcement, technological innovation, financial monitoring, and international intelligence sharing form an integral part of the cross-domain strategies (Fraih, 2026).

There is a need to grasp the set of mechanisms at the intersection of hybrid warfare and criminal networks as a fundamental step in developing policies and strategies appropriately. Research needs to explore the role of criminal organisations in hybrid campaigns, technological and financial innovations that prosecute them, vulnerabilities that they exploit and the international cooperation that is needed to tackle the hybrid threats. Furthermore, understanding these interactions can help shape the development of law, intelligence-sharing and multi-sector policy solutions that can build state resilience and improve global security. This research is designed to give an in-depth look at the relationship between hybrid warfare and transnational criminal networks (TCNs), identify new trends, discuss the threat to international security, and present policy recommendations. The study problematizes the operation structures, technological enablers, and strategic use of crime networks, thereby enhancing the understanding of the multidimensional nature of current hybrid conflicts. This highlights the importance of coordinated international responses, proactive intelligence gathering, technological innovations, and robust legal mechanisms to address the evolving threats in relation to the convergence of hybrid warfare and Organized Crime (Osman, 2026; Ding, 2026; Mehmood, 2026; Stavropoulou, 2026; Zandieh, 2026; Fraih, 2026; Maritan, 2026).

Literature Review

Conceptualizing Hybrid Warfare

Hybrid warfare is now described in a wide variety of ways, most of which revolve around a notion of warfare that is adaptive, complex, and uses a spectrum of military and non-military means to accomplish its strategic ends. While early scholarship focused solely on the blending of conventional and irregular warfare, recent research has included cyber warfare, information warfare, assassinations, and the use of transnational criminal networks as integral pieces of the hybrid warfare puzzle (Bukhari, 2026; Ghimire & Neupane, 2026). In hybrid warfare, the use of multiple layers of conflict, including peace and war, combat and non-combat, involves using multiple domains simultaneously, with the intent of reducing the strength of the opponent while leaving the option of a legal (and military) response unclear (Osman, 2026).

Exploiting Vulnerabilities in Open Societies

Hybrid warfare is frequently directed towards structural weaknesses within pro- open societies. Hybrid actors can mount disinformation campaigns; carry out cyberattacks; create economic pressure; conduct proxy wars; and influence politics – all without resorting to conventional militarization. Aggressors can plausibly deny when they act aggressively and international attribution is difficult, leading to difficulties in coordinated response and slowing down policy action (Ding, 2026).

Evolution of Organized Crime in the Global Era

The nature of organized crime is evidenced by research to be a transnational business that has been spuriously adaptive. Hierarchical companies are becoming more and more decentralized networks that can easily form alliances, generate new revenues, and quickly adapt to digital communication technologies. Presently, modern criminal organizations are concurrently involved in the trafficking of narcotics and arms, cybercrime, money laundering, the smuggling of humans, anti-

environmental offences and financial fraud with an operational sophistication that synergizes with the goals of hybrid warfare (Motaung & Ani, 2026).

Crime–Conflict Convergence

The legal and definitional distinctions between acts of terror, insurgency, organised crime and hybrid warfare have become confused, as detailed in the idea of 'crime–conflict convergence' (CCC). According to scholars, more and more criminal organizations are collaborating with hybrid actors, providing them with resources, intelligence, logistics, and operational support, all for the greater benefit of criminal organizations and hybrid actors. This convergence serves to increase the operational efficiency of hybrid campaigns but also provides criminal networks with protection, market access and legitimacy; it allows to merge the crimes into broader geopolitical conflicts (Stavropoulou, 2026).

Cybercrime as a Force Multiplier

The role of the cybercriminal groups has been highlighted as a key player in the literature on hybrid warfare. Ransomware profits, DDoS attacks and advanced malware campaigns of today cost billions of dollars a year and are often linked to geopolitical goals. Many ransomware groups are based in jurisdictions with implied protections, and could be attacking foreign governments and corporations without having any repercussions in their home countries. Access of these cyber-enabled capabilities makes criminal networks efficient force multipliers for hybrid campaigns and enable to deliver disruption at minimal costs (Kumar, 2026).

Financial Networks and Illicit Economies

Unlawful money transfers are a key enabler for hybrid and criminal activities. Research highlights the role of money laundering, shell companies, off shore financial centers, trade-based money laundering, cryptocurrencies and digital payment platforms in obscuring financial transactions and evading sanctions. These mechanisms enable criminal networks to source funds for proxy groups, fund hybrid operations, and expand transnational operations without getting caught. These networks, due to their financial flexibility, amplify the strategic value in hybrid conflicts (Maritan, 2026).

Information and Influence Operations

Information warfare has turned one of the key areas of cybercrime-assisted hybrid warfare. Criminal groups also run Disinformation Campaigns via fake social media, botnets, hacked databases and influence operations. Criminal activities with financial motives can interact and intertwine with ones of a political nature, when there is an economic advantage or when it has a strategic interest for the financial criminals, includes social and political football (Ustiashvili, 2025). This gives an example of how organised crime may come into contact with state or proxy hybrid agendas and thus help increase destabilisation.

Corruption and Governance Vulnerabilities

A key enabler that links organised crime and hybrid strategies is corruption. Poor government institutions, a weak political system, inadequate oversight and the lack of judicial independence provide criminal groups with scope to breed and integrate within public institutions. Infiltrated into the country, these networks enable outside actors to infiltrate domestic decision-making processes, reduce the effectiveness of institutions, and enable hybrid operations (Fraih, 2026). This confirms the need to reform governance as well as the anti-corruption mechanism to address hybrid threats.

Technological Enablers of Hybrid Operations

Technology is a force multiplier for criminal networks and hybrid actors. AI, machine learning, the use of commercial drones, blockchain, encrypted communications, and dark web marketplaces boost operational capabilities. Through these technologies, anonymous financial transactions, automated cyber attack, intelligence collection and cross-border coordination of influence operation are made possible. Scholars highlight that technology offers capabilities that enhance states' countermeasures but, at the same time, lowers the barrier to entry for hybrid actors and criminal organisations (Gelot & Khadka, 2026).

Gaps in Current Scholarship

Even if there has been some progress in studying hybrid warfare and organized crime separately, many studies do not methodologically analyze their confluence. Studies tend to either examine cyber threats, hybrid strategies or criminal networks, but generally do not do all three and limit comparative or regional analysis. Furthermore, there is limited research about the role of criminal networks in actively facilitating state-sponsored hybrid operations, whether cyber-based finance, logistics, sanctions evasion or disinformation campaigns. However, to create effective integrated policy frameworks (Xu et al., 2026), the gaps need to be addressed.

Interdisciplinary Approaches

A comprehensive understanding of the hybrid–crime nexus requires interdisciplinary methodologies, which include an understanding gained from international relations, security studies, criminology, cybersecurity, economics, intelligence analysis, and law enforcement fields. These can help to shape comprehensive countermeasures against multi-faceted threats and give a picture of how hybrid warfare and the criminal cooperative can be approached in the operational, technological, financial and legal aspects. When researchers can connect the dots across discipline silos, they might make evidence-informed policy recommendations to combat risks from the hybrid/criminal nexus (Osman, 2026).

Implications for Policy and Security

According to literature, hybrid threats can only be addressed through co-ordinated policy reactions at the international level, technological investments, intelligence sharing mechanisms and regulatory changes. Effective strategies start with the understanding that criminal syndicates and hybrid operations are constantly evolving and need to consider the need for a cohesive response of law enforcement, military, intelligence and regulatory bodies, to the nature of these syndicates and their operations. Experts call for anticipatory threat assessments, advanced technological solutions, and legal measures to address threats posed by criminal networks in the service of hybrid warfare goals (Stavropoulou, 2026).

Research Methodology

The methodology in this analysis is qualitative, with analysis of secondary data sources that provide an in-depth look into the interaction between hybrid warfare and criminality transnational networks. In hybrid conflicts, which have political, military, economic, technological, legal and criminal dimensions, a qualitative approach makes it possible to deepen or gain an understanding which cannot be gained by quantitative approach only. Peer-reviewed academic literature, strategic studies, policy reports, government publications, think tank analyses and documented case studies on hybrid conflicts throughout Europe, the Middle East, Latin America and Africa, and in cyberspace, were all used to collect the data. Descriptive and analytical methods were used to determine the trends of collaboration, the way of operation and criminogenic goals of criminal organizations involved in hybrid campaigns. Comparative case study analysis also yielded insights on contrasting state conditions of governance, law enforcement response, technological adoption,

and state-criminal relationships in different kinds of geopolitical contexts. The study looks at the "force multipliers" that criminal networks may provide in a hybrid war, and the functions of cybercrime, money laundering, arms trafficking, sanctions evasion, and disinformation. Some limitations include that most of the literature comes from secondary sources and results of the situation may be subject to reporting bias and that hybrid threats are continually changing and not entirely captured in the literature.

Discussion

The Evolution of Hybrid Warfare

Hybrid warfare is a paradigm shift in conflicts where the enterprising elements of war are being combined with non-military paramounts to reach strategic military goals without resorting to conventional warfare. Hybrid strategies have elements of both interstate and non-state actor conflict, and involve military action, cyberspace attacks, information warfare, economic pressure, covert action by both sides, proxy players, sabotage, and organized crime. The goal is to undermine and weaken opposition institutions, to create inertia and uncertainty with decision-making, and to secure strategic advantages without a conflict or to avoid an open conflict (Yom, 2026). Hybrid warfare operations are still very much about plausible deniability and states are able to carry out destabilising operations via the use of proxies, private military companies, hackers, and criminal networks. These strategies were further accelerated in these last years by the emergence of the digital revolution, allowing to attack assets such as critical infrastructure, financial systems, healthcare networks, and communication platforms with relatively small investments and strategic impact (Yu et al., 2026).

Criminal Networks as Strategic Enablers

The role of criminal groups has become a major force multiplier in the framework of hybrid warfare. They have wide-ranging transnational logistical networks built up over decades of unlawful operation such as drug routes, human smuggling networks, maritime shipping routes, financial network and document forgery systems. They operate extensive corruption rings in the Police, Customs, banking and other political institutions through which hybrid actors can evade laws and hide behind suspicious operations (Bukhari, Khan, et al., 2024). Criminal groups are also known for their financial scale, which makes laundering money on a global scale estimated at between US$800 Billion and US$2 Trillion per annum, rival to some States. With these resources, advanced technologies can be acquired, skilled personnel can be recruited, weapons can be purchased, and sustainability can be achieved.

Cybercrime in Hybrid Operations

Cybercrime plays a major role in the hybrid warfare strategies. Ransomware groups, cybercriminal enterprises and hacking syndicates engage in sophisticated cyber attacks targeting hospitals, energy providers, transportation systems, financial institutions, and government agencies. A significant amount of criminal profit is derived from these operations alongside generally doing significant damage to the public trust in the state institutions (Loginova, 2026). Cybercrime enables intelligence in addition to blackmail and sabotage and disinformation activities. Additionally, encrypted communication, anonymisation tools and cryptocurrency payments add to the overall security of the operation of hybrid actors and criminal co-conspirators.

Illicit Financial Networks and Economic Manipulation

Economics is an integral part of the hybrid conflict. Criminal networks take advantage of gaps in regulation, enforcement of financial sanctions, and banking systems around the globe to fund hybrid campaigns. Money laundering methods include the manipulation of shipping documents,

shell corporations, falsified shipping documents, and trade-based money laundering, all of which make it possible for illegally-gained money to flow through the system unnoticed. A non-governmental application of cryptocurrencies is the possibility of using them by anonymous entities to acknowledge cross-border transactions, which allows for the circumvention of economic sanctions in sanctioned states. Such illicit funding allows for proxy activities, bribes, and campaigns over the long term with no clear tailback (Smolny, 2016).

Information Warfare and Propaganda

The new trend of information operations has increasingly become a weapon of the hybrid actors. Routine access to pirated databases, botnets, social media manipulation, and the spread of malware are common activities of criminal networks used to assist mayhem campaigns. Fake accounts, disinformation, and similar attacks can disrupt political processes, impact political elections, and erode public trust through automated social media accounts, targeted phishing campaigns, and the creation of fake profiles. Criminal enterprise is blending with hybrid conflict, as finance-driven actors take on and work alongside politically motivated actors when shared strategic or economic interests are involved (Yalçınkaya, 2025).

Proxy Actors and Operational Flexibility

Proxy actors are a key feature of hybrid warfare to give plausible deniability. Criminal organisations, private military companies, local militias and separatist movements give operational capacity without any obvious state participation. These proxies are used to transport weapons, money, prohibited items, and intelligence across international boundaries, typically with less risk of international accountability. These relationships, however, are always transitory, allowing criminal groups to achieve a degree of freedom of operations and a material payoff, while the hybrid entities enjoy access to their network, corruption and logistical support (Fattah, 2026).

Corruption as a Facilitating Mechanism

The dynamics of corruption is a significant enabler connecting criminal networks and hybrid warfare. Poor government, inadequate judicial independence, political instability and lack of regulation provide space for infiltration. Smuggling, money laundering, and sanctions evasion are made easier by criminal groups operating with little scrutiny due to bribery of officials at the border, customs, and financial institutions. When foreign investment takes place in the presence of corruption, tax revenue is further affected, and the public lose trust, thus sustaining an environment of favours for hybrid and creating cycles of instability.

Emerging Technologies and Future Threats

The hybrid actors can exploit a wide range of new operational tools as a result of the rapid technological innovation. Drone operations in commerce are used for surveillance and intelligence gathering, delivery of weaponry and carrying of contraband. AI can power automated cyberattacks and allows for predictive threat analysis and quick data processing. Industrial systems, healthcare networks, transportation as well as energy infrastructure are part of the attack surface that can be compromised via blockchain and privacy-enhancing cryptocurrencies that can allow covert financial transactions. Although a new technology, quantum computers could eventually break encryption protocols and create new dangers if put in the possession of a state actor or criminal. These technologies boost both the sophistication and the potential impact for hybrid campaigns (Liyang et al., 2020).

Geopolitical Implications

Geopolitically, there are great consequences for the overlap of hybrid warfare and criminal networks. Hybrid campaigns can over throw States, affect elections, stifle change in economics

and infrastructure, and affect public perception. Criminal networks compound these effects, offering expertise, finance and operational strengths. These are especially susceptible in areas where there are weak or unstable government or widespread corruption. International actors are increasingly acknowledging the need for a whole-of-society approach, involving the co-ordination of law enforcement, military arrangements, intelligence, financial regulation and public-private cooperation to address hybrid threats.

Policy and Strategic Considerations

It is important to take multidimensional approaches with regards to counter-hybrid strategies. Policy should incorporate cyber security and regulatory, border, intelligence sharing, and counter-corruption elements. Enhanced international co-operation is needed with mutual legal assistance treaties, harmonisation of legislation and joint investigations of crime. To disrupt criminal support structures, public-private partnerships between the government and technology businesses, financial institutions, and logistics providers are essential. By proactively monitoring, threat modeling, and scenario planning, we can increase resilience, without losing sight of ethics and the preservation of civil liberties. In the 21st Century, hybrid warfare shows that criminal networks are not any longer an ancillary player, in any case they are one of the key enablers of strategic operations. By providing force multiplying capabilities to hybrid actors, they are indispensable as force multipliers based on their financial capabilities, technological capabilities, operational flexibility and corruptible/malicious infrastructure. Examples of convergence of criminal enterprise and hybrid conflict include cybercrime, financial crime, proxy operations and information manipulation. Interdisciplinary solutions, and even legal ones, are required to solve these issues, with the inclusion of several different aspects ranging from law enforcement, international cooperation, technological innovation, anti-corruption efforts, strategic policy design. Both States and international institutions should be adaptive to new and emerging hybrid threats to protect global security, economic stability and good governance.

Findings / Results

Criminal Networks as Strategic Actors

The results of the study show that, apart from being profit-seeking enterprises, organized criminal groups have transformed into one of the actors strategically important to the international security environments. These networks are financially well-resourced, have transnational infrastructure, technical know-how, and flexibility in operating. These enable state actors or nonstate hybrid actors to accomplish their goals without military involvement by offering assistance with logistics, communications and concealed sources of funding. Weak governance, weak law enforcement capabilities, and gaps between jurisdictions are leaving criminal networks with freedom to operate and some plausible deniability, while keeping the risks for hybrid actors low (Bukhari, Khan, et al., 2024).

Cybercrime as a Force Multiplier

Cybercrime is the fastest growing area of interplay for criminal groups and hybrid warfare actors. Dual benefits, such as revenue generation and strategic disruption, from ransomware groups, cyber extortion networks, darknet marketplaces, and cryptocurrency-based financial systems. Cybercriminal operations provide an indirect means for hybrid actors to target critical infrastructure, such as health care systems, energy grids, and transportation systems. Hybrid actors can function anonymously and create political, economic and social chaos, all while continuing to operate beyond borders, as their ability to do so has been fundamentally changed with the advent of digital means of projection (Loginova, 2026).

Illicit Financial Flows and Money Laundering

Financial networks continue to be a key enabler of hybrid operation. Money laundering, shell companies, offshore property, trade finance, and cryptocurrency are tools used by criminal organizations to hide their criminal conduct, as well as provide sanctions evasion, hidden funding, and strategic influence. Estimates of the amount of money laundered around the world vary from US$800 billion to US$2 trillion; this is a significant amount of money for criminal networks to exploit in hybrid conflicts. These fund transfers enable procurement of weaponry, recruitment of specialized personnel, sustained hybrid campaigns and technology acquisitions, adding more to the strategic value of the criminal actors (Malik, et al., 2024).

Corruption and Institutional Vulnerabilities

One area that invariably becomes a vulnerability to be targeted by both criminal networks and hybrid actors is corruption. The activities of criminal organisations make their way into state mechanisms, influence regulatory frameworks and undermine law enforcement in the context of weak governance, lack of judicial independence, financial weaknesses and poorly-regulated institutions. Bribes and facilitation payments enable hybrid actors to evade security checks, smuggle illegally obtained goods, and communicate with groups illicitly. Hybrid strategies are more likely to be effective when institutional corruption is widespread, as the corruption helps these crimes take place with impunity (Yu et al., 2026).

Technological Innovation and Operational Capabilities

New and emerging technologies have dramatically increased the capabilities of criminal networks, and hybrid actors. Sources of AI, encrypted communications, commercial drones, blockchain and marketplaces and darknet enable fast, flexible and widespread operations to be conducted in complete anonymity. AI allows for automated cyberattacks, behavior analysis, as well as predictive logistics, with the drones specifically being used for surveillance, smuggling, and sabotage. Use of encrypted communication platforms and decentralized financial systems makes it harder to detect, more anonymous, and can give safer alternatives for operational coordination (Liyang et al., 2020).

Globalization and Transnational Reach

Criminal networks now operate on a global level. International trade, financial integration and digital connectivity enables the movement of persons, goods and money to speed up faster across borders. Smuggling routes extend across many continents and cyber operations can take place in any region of the world and against critical systems. This interconnectedness makes criminal networks even stronger in terms of their strategic value in the context of hybrid warfare, where the interdependence can be used to pursue political, economic and military ends (Smolny, 2016).

Targeting Civilian Infrastructure

Today's forms of hybrid warfare are becoming more focused on civilian targets than military targets. Because of the uncertainty, economic losses, and politically pressure it causes, hospitals, transportation networks, banking systems, electric grids, educational institutions, and governmental databases have all become potential targets. Criminal networks support such operations with logistical, technical services and covert financial channels, thereby increasing the impact and effectiveness of the attacks on civilians targets (Yalçınkaya, 2025).

Fragmentation of Security Frameworks

The players mentioned institutional failure as one of the challenges to effective responses to hybrid threats. These are likely to have gaps that hybrid actors exploit, especially when operating in isolation and using their own architectural approaches, such as those by military organizations,

intelligence agencies, law enforcement bodies, financial regulators, and cybersecurity authorities. The inter-agency coordination processes are not effective, there is a lack of information sharing between agencies; and a lack of operational efficiency of the agencies and the prosecution of cross-border crimes is hamper. Integrated frameworks which include security, financial, legal, and technological institutions within a single strategy are vital in the process of successful mitigating hybrid threats risks (Fattah, 2026).

Integration of Cybercrime, Finance, and Hybrid Operations

More often than not, hybrid warfare operations combine cybercrime with illegal financial and conventional criminal activities. Cyberattacks, ransomware, money laundering, human smuggling and document fraud are all part of a central supporting state-sponsored or politically motivated campaign. Criminal networks also serve as facilitators, offering technology, operational flexibility and plausible deniability. By joining in with hybrid campaigns, they also expand their reach and effectiveness and have become more of an integral part of a criminal network than mere cases, becoming strategic partners, in essence (Bukhari, et al., 2024).

Implications for Security Policy

The report indicates that countering hybrid threats and responding to them necessitates a multi-dimensional approach, encompassing the technological, financial, institutional, and operational aspects. This requires integrated national and international approaches and will need to involve law enforcement, military preparedness, financial regulation and regulation, cyber resilience, intelligence sharing, anti-corruption and public private partnerships. It is also essential to take preventive steps, including keeping an eye on new technologies and improving governance structures, to minimize vulnerabilities that are exploited by hybrid actors and criminal networks (Yu et al., 2026). This research shows that hybrid warfare and criminal networks are symbiotic. Criminal groups offer invaluable credits, logistical support, financial outlets, as well as corruption that contributes to the success of hybrid campaigns. Examples of strategic competition that have evolved include cybercrime, illicit financial flows, and attacks on civilian infrastructure. Solutions to meet these challenges demand an integrated and interdisciplinary strategy with a focus on national security, law enforcement, financial oversight, cyber defence and international cooperation to create resilience against hybrid actors and their criminal partners.

Conclusion

The current security landscape has resulted in a new paradigm of hybrid warfare (HW), one that has helped to erode the lines between war and peace, military and civilian activities, and state and non-state actors, which are now characterized by the intertwining of HYBRID WARFARE and transnational criminal networks. Conflicts are no longer fought exclusively with traditional military means – but using multifaceted and integrated strategies involving cyberattacks, information manipulation, economic coercion, proxy organisations, organised crime, illicit finance and technological disruption. Criminal network has become an essential part of these campaigns, providing a time-tested and versatile logistics, technological competency and financial power. The research shows that organized crime has gone from a money-making exercise to a means for hybrid warfare. Criminal networks are used to support cyber activities, sanctions, illicit financial transactions, arms trade, intelligence and disinformation. They are decentralised, operate globally and can exploit governance deficiencies and lead to a geopolitical benefit of state and non-state actors with a plausible deniability.

Cyber operations are a primary method of hybrid operations. Bad guys profit enormously from ransomware groups, darknet marketplaces, cryptocurrency laundering websites, and cyber-extortion marketplaces while causing significant disruption. The types of attacks being used

against energy grids, hospitals, financial systems, transportation and telecom networks, and even government databases are proof of the impact non-traditional actors can have—s effects that are similar to what we see with traditional military attacks. IFF further boosts the strategic capabilities of criminals. The use of trade-based money laundering, shell companies, accounts abroad, digital assets and informal value transfer systems facilitates subterranean trade, the financing of other players, circumvention of sanctions, and ongoing hybrid operations. This shows that financial crimes are not only an issue of law enforcement, but that financial crimes have become part and parcel of national and international security strategy.

Corruption is always found to be a major enabler in the nexus between organized crime and hybrid warfare. The presence of weak governance, lack of regulation, political instability and low judicial independence enable criminal networks to be able to infiltrate institutions, influence policy-making, and to erode the rule of law. This susceptibility allows for space to be given to hybrid actors to influence and disrupt governance mechanisms and achieve strategic goals without having to act openly or transparently. Criminal networks have been greatly enhanced in their capacity of operations by technological innovation. Things like artificial intelligence, blockchain, encrypted communications, commercial drones, cloud computing, and the IoT increase reach, speed, and anonymity that can be used by more sophisticated hybrid actors for operations that largely go undetected. Such technologies offer their own economic and social advantages, but also present opportunities that can be abused for strategic and criminal reasons.

Issues of fragmentation of institutional responses are still very much present. Military groups, intelligence services, cybersecurity agencies, law enforcement, financial and customs authorities can all be widely autonomous and unaware of each other, areas ripe for hybrid players to target. These efforts need to be coordinated, with enhanced surveillance systems and well-functioning response mechanisms, in order to ensure a unified effort. Addressing these multidimensional threats will require cooperation between countries. Criminal operations span the entire world and often multiple jurisdictions are impacted by hybrid simultaneous campaigns. As mitigation becomes a tool for sustainable action, intelligence sharing, harmonised legal measures, harmonised and coordinated implementation of sanctions, joint cyber defense efforts and transparency in financial controls play an important role. The hybrid warfare and criminal networks are a self-reinforcing phenomena. However, these challenges demand a combination of national and international strategies that address the issues of security preparedness, financial regulation, technological resilience, anti-corruption and robust governance. In an age of complex, transnational hybrid threats, strengthening democratic institutions, cyber security and international cooperation will be key for decreasing vulnerabilities, maintaining strategic stability and ensuring global security.

Recommendations

Integrated National Security Strategies

Governments need to establish a national approach, whereby all domains of defence, law enforcement, intelligence, cybersecurity, financial regulation, customs and judicial are integrated into a single approach on hybrid threats. Interagency coordination needs to be formalized, improve communication, speed up response time and ensure the coordinated and synchronized use of resources so as to minimize gaps which criminal networks and hybrid actors are able to exploit.

Enhanced International Intelligence Sharing

States should build-up mechanisms to share information on organised criminal networks, cyber threats, illicit financial flows, sanctions evasion, and emerging hybridities in real-time. The capacity to function in coordination with my partners throughout the region will enhance early-

warning capabilities, facilitate coordinated investigations and enhance the effectiveness of transnational operations.

Cybersecurity Resilience
The important thing is to invest in robust digital infrastructure, incident response capabilities and workforce training. Governments need to adopt improved cybersecurity requirements in sensitive sectors, implement contingency plans and encourage public-private cooperation to identify, deter and respond to hybrid cyber activities.

Financial Transparency and Oversight
Anti-money laundering (AML) and counter-terrorism financing (CFT) laws and regimes need to be tightened. Governments need to keep an eye on shell companies, registers of beneficial owners, cross-border transactions and virtual assets service providers in order to limit the use of financial systems to perpetrators of hybrid warfare.

Regulatory Frameworks for Emerging Technologies
New regulations around cryptocurrencies and decentralized finance are needed that strike the balance between encouraging innovation and ensuring security. With regard to financial intelligence units, legislative backing and, at a technical level, their capabilities should be improved to enable monitoring of digital money transfers that are carried out by the hybrid actors or criminal organisations.

Anti-Corruption Reforms
Corruption is an eroder of state resilience towards hybrid threats. Increasing the independence of judges, creating more responsible public sector, making public procurement more transparent and the protection of whistleblowers will minimize the opportunities for the infiltration and manipulation of hybrid actors.

Specialized Law Enforcement Capabilities
There is a need for agencies to grow their capabilities in cybercrime investigations, digital forensics, blockchain analysis, AI-assisted intelligence and open-source intelligence (OSINT). Continuous professional development is imperative to stay up-to-date on the ever-changing tactics used by criminal networks and hybrid actors.

Strategic Communication and Public Resilience
Governments should put in place measures to combat disinformation and influence campaigns. Media literacy education, open communication practices, quick fact checking systems, and awareness campaigns will boost resilience of society to face hybrid attacks based on information.

International Legal Harmonization
International bodies should encourage harmonized laws on cybercrime and digital evidence, extraditing cyber criminals, sanctions enforcement and mutual legal assistance. Harmonization limits gaps between the jurisdictions that transnational criminal networks exploit, and enhances the effectiveness of multinationals efforts.

Modernized Border Security
Biometric identification, AI-powered surveillance, drones, and cutting-edge cargo inspection systems must be used to bolster Borders. These measures serve to disrupt illegal trafficking, arms smuggling and cross-border criminal networks that add to the capabilities of hybrid warfare.

Public-Private Partnerships

Collaboration between public institutions, academia, technology companies, financial institutions and civil society should be promoted in the government. Partnerships offer specialized expertise, innovative technology and threat intelligence, which further bolsters capacity on the national and international level to address hybrid threats.

Research on Emerging Technologies

The field of 3D printing can explore future research areas such as AI, quantum computing, autonomous systems, synthetic media, and advanced encryption. An understanding of the security implications of these technologies will help policymakers assess how to counter them both proactively and reactively as well as help them prepare for potential security threats in strategic planning.

References

Bukhari, S. R. H. (2026). Between Brotherhood and Betrayal: A Historical Analysis of Afghanistan–Pakistan Relations. *International Social Research Nexus (ISRN)*, *2*(1), 1–8.

Bukhari, S. R. H., Khan, T. U., Khan, N., Khan, A. U., Noreen, S., Haq, I. U., Ullah, T., & Khan, E. (2024). China's Trade Relations with the United States Matrix of Conflict and Cooperation. *Research, 9 (2)*, 263–284.

Bukhari, S. R. H., Malik, S. M., & Mahmood, M. A. (2024). Chinese BRICS: Contamination of US-led Neoliberalism. *Pakistan Social Sciences Review*, *8*(2), 320–331.

Ding, J. Z. (2026). A Dialogue on East-West Views of "Cosmopolitanism." In J. Z. Ding, *Real Being and Cultural-Humanistic Phenomena* (pp. 57–98). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-15424-8_2

Fattah, A. (2026). China's strategic approach to the Persian gulf: Balancing relations between Iran and Saudi Arabia. *International Politics*. https://doi.org/10.1057/s41311-025-00746-1

Fraih, Z. (2026). Balancing Act: Algeria's Foreign Policy amidst US-China Strategic Competition. *المجلة الأكادمية للبحوث القانونية والسياسية*, *10*(1), 90–117.

Gelot, L., & Khadka, P. B. (2026). Combat Legitimacy and Robust Peace Operations: Calibrating Military Protection of Civilians. *Journal of Intervention and Statebuilding*, *20*(1), 90–113. https://doi.org/10.1080/17502977.2025.2561418

Ghimire, A., & Neupane, M. S. (2026). Back home, beyond borders: A bioecological study of returnee public health scholars in a globalized health system. *Globalization and Health*, *22*(1), 34. https://doi.org/10.1186/s12992-026-01201-3

Kumar, S. (2026). Artificial Intelligence and the Nuclear Deterrence Paradox: Rethinking Deterrence in South Asia and the Middle East. *Journal of World Affairs: Voice of the Global South*, 29769442251410646. https://doi.org/10.1177/29769442251410646

Liyang, W., Jiayi, W., & Qian, L. (2020). Critical Discourse Analysis of Sino-U.S. News Reports on Trade War: A Corpus-based Comparative Study. *English Language, Literature & Culture*, *5*(3), 84. https://doi.org/10.11648/j.ellc.20200503.12

Loginova, A. (2026). Co-optation for authoritarian regime stability in post-war Russia: New mapping approach. *Democratization*, 1–25. https://doi.org/10.1080/13510347.2026.2636049

Maritan, M. (2026). *Austria Neglecta*: Rethinking the Theory of Nationalism between Acton, Mazzini, and the Habsburg Legacy. *The European Legacy*, 1–34. https://doi.org/10.1080/10848770.2026.2645810

Mehmood, Z. H. (2026). AI, Information and Maritime Security: Implications for Global Trade and Geopolitical Competition. In F. Roumate (Ed.), *AI, Information, and Global Dynamics* (pp. 137–156). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-13528-5_10

Motaung, P. G., & Ani, K. J. (2026). AU-UN peacekeeping relations and inherent gender issues. *International Journal of Studies in Inclusive Education*, *1*(si1), 50–53.

Osman, K. F. (2026). 4 Evolving Dynamics. *Yemen at the Crossroads: Crisis and Reconstruction*. https://books.google.com/books?hl=en&lr=&id=rVHGEQAAQBAJ&oi=fnd&pg=RA2-PA2022&dq=What+challenges+face+Saudi-led+coalitions%3F&ots=ut4mLMGpZb&sig=snLrBpf_og5RDXvj60Bwlq5LWEg

Smolny, D. (2016). Current challenges to the non-proliferation regime: Iran and North Korea. A summary of professor Harnisch' lecture. *Security and Defence Quarterly*, *10*(1), 21–34. https://doi.org/10.5604/23008741.1215400

Stavropoulou, I. (2026). *Are Multidimensional Environmental Changes Threats to National Security? An Analysis of National Security Policies of Schengen Area Countries*. https://www.diva-portal.org/smash/record.jsf?pid=diva2:2054846

Ustiashvili, S. (2025). Bridging alliances: The political, economic, and strategic impact of President Trump's Saudi Arabia visit on U.S.-Arab relations. *Israel Affairs*, 1–13. https://doi.org/10.1080/13537121.2025.2583223

Xu, C., Zhang, J., & Zhang, Y. (2026). *China's New-Era Maritime Security: A Holistic National Security Framework*. Paths Publishing Group. https://books.google.com/books?hl=en&lr=&id=wonAEQAAQBAJ&oi=fnd&pg=PP1&dq=Public+Health+as+National+Security:+Rethinking+Global+Health+Governance+in+an+Era+of+Geopolitical+Competition&ots=SKfa9qTtZl&sig=5K2QR64gfc92sHz09Oc0kybLFrg

Yalçınkaya, F. (2025). *Crafting Compendiums, Making Law: Ottoman Legal Compendiums And The Reconfiguration Of Legal Authority In The Seventeenth Century* [PhD Thesis]. https://research.sabanciuniv.edu/id/eprint/53076/

Yom, S. (2026). Domestic Politics and Foreign Policy Change: The Gulf Model in Saudi Arabia and the United Arab Emirates. *Global Studies Quarterly*, *6*(2), ksag070.

Yu, C.-H., Shi, Y., Lee, C.-C., Zhao, J., & Li, X. (2026). Climate finance as a catalyst for peace. *Climate Policy*, 1–15. https://doi.org/10.1080/14693062.2026.2645656

Zandieh, A. (2026). Artificial intelligence, economic inequality, and the financial hurdles to sustainable peace: Navigating the interconnected challenges of the 21st century. *Social Sciences & Humanities Open*, *13*, 102687.