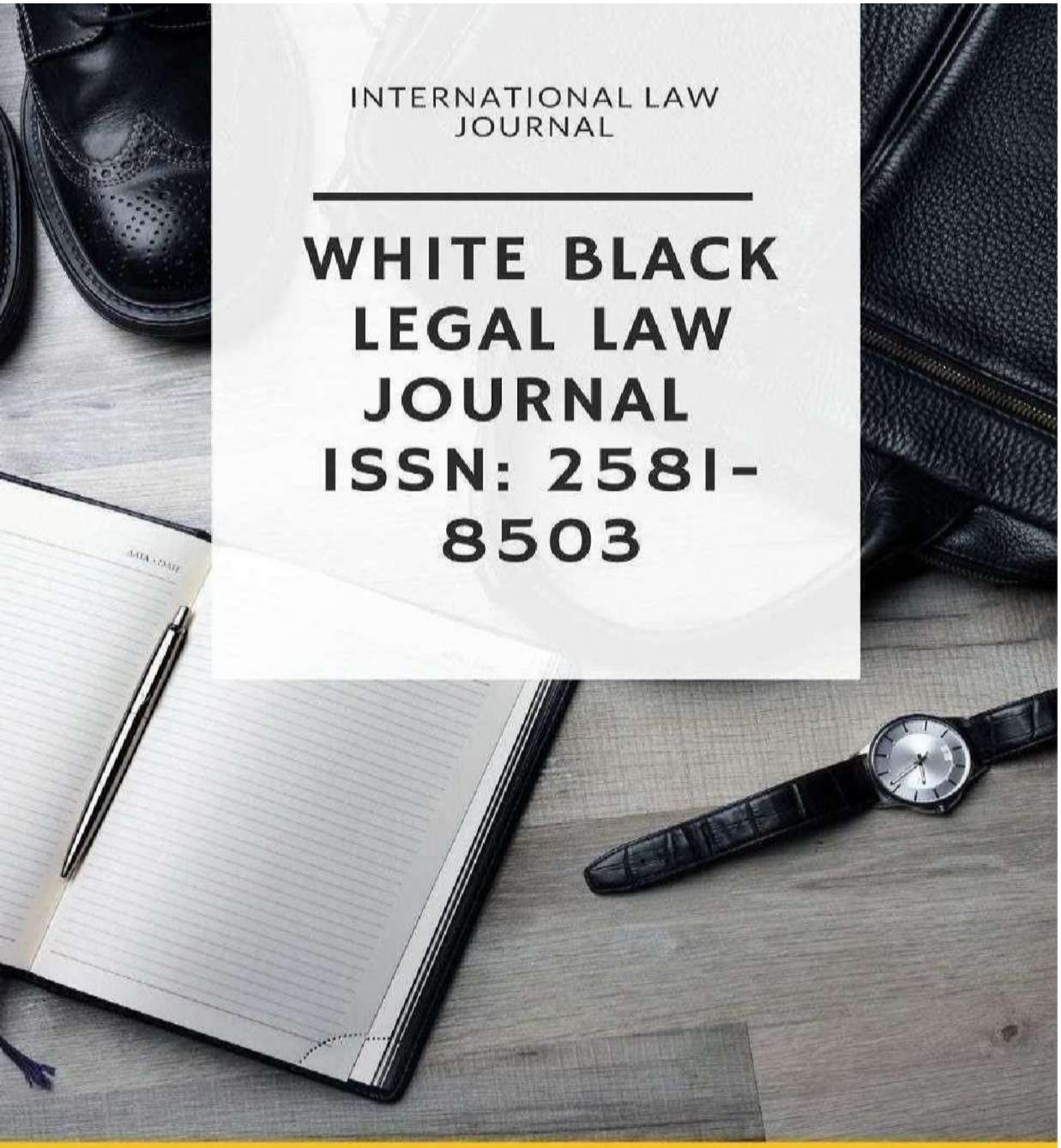

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and

refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | Dec 2024 ISSN: 2581-8503

DRONE, ROBOTS AND CYBER WARFARE

AUTHORED BY - PALAK BANSAL

ABSTARACT

Modern warfare has undergone a revolution with the introduction of drones, robotics, and cyberwarfare. This has presented military forces across the globe with new problems and capabilities. With real-time data and imagery that help with situational awareness and decision-making, these technologies have greatly improved intelligence, surveillance, and reconnaissance capabilities. Furthermore, by enabling pinpoint strikes on enemy targets, drones and robots have reduced collateral damage and civilian casualties. The application of sophisticated cyber capabilities in the field of cyberwarfare has made it possible to launch focused attacks on adversary systems and infrastructure, impairing their capacities and operations.

However, there are moral and legal issues with the employment of robots, drones, and cyberwarfare. The main concerns that need to be addressed are targeted killings, privacy rights, weaponry autonomy, and civilian casualties. To allay these worries, adherence to ethical standards, human rights doctrine, and international humanitarian law is crucial.

INTRODUCTION

Cyberwarfare, robotics, and drones are all essential parts of contemporary military and security plans. Each contributes differently to the way that modern warfare is shaped.

Unmanned aerial vehicles, or drones: Drones are pilotless aircraft that are controlled remotely by a human operator. They can be applied to combat, surveillance, and reconnaissance tasks. Some drones are now able to execute precise missile or bomb strikes, demonstrating the rising sophistication of drone technology.

Robots: Robots are autonomous or semi-autonomous devices used in warfare that are capable of carrying out a range of duties, including bomb disposal and reconnaissance. They are able to function underwater, in the air, and on land. Military robots are intended to lower hazards and improve human soldiers' capabilities.

Cyberwarfare: Cyberwarfare is the use of computer technology to attack or compromise an enemy's information systems. This can involve propagating false information, breaking into computer networks, or taking down vital infrastructure. Because cyberwarfare may be used to target political, economic, and military interests, it has become a major issue for governments everywhere.

Drones, robots, and cyberwarfare all symbolise how modern warfare is changing and how technology is becoming more and more important. Although these tools have the potential to improve military capabilities, they also bring up difficult moral and tactical issues regarding the nature of conflict and the use of force.

I. DEVELOPMENT OF DRONES

Over the years, there has been a tremendous evolution in the creation of unmanned aerial vehicles, or drones. Drones have become into sophisticated instruments with a wide range of uses since they were first employed for surveillance. Here is a quick synopsis of their evolution:

Early History: The idea of drones was initially introduced in the early 1900s. The earliest known application of an unmanned aerial vehicle was during Austria's 1849 raid on Venice, when unmanned balloons carrying explosives were used as weaponry. More useful advancements, though, started to appear in the early 20th century.

World War I: Drone technology was tested by the United States and the United Kingdom during the Great War. Charles Kettering created the Kettering Bug, which is an early example. It was an autonomous aircraft intended to deliver explosives to adversaries.

World War II: During the conflict, drone usage grew, mostly for target practice and as decoys. The first UAV to be mass-produced in history was the Radioplane OQ-2, which was developed in the United States. In order to increase drone accuracy, actress and inventor Hedy Lamarr created a radio guiding system, which she also contributed to drone technology.

Cold War Era: Drone technology advanced and drones were utilised for reconnaissance at this time. Drones such as the AQM-34 Ryan Firebee, which was widely utilised for reconnaissance flights over Vietnam, were created by the United States.

Modern Era: Drone technology has advanced quickly in the modern era. Nowadays, drones are employed for many different tasks, such as aerial photography, agriculture, disaster relief, combat operations, monitoring, and reconnaissance.

Overall, the development of drones has been driven by advancements in technology and the evolving needs of military and civilian users. Drones have become an integral part of modern warfare and are likely to continue to evolve as technology progresses.

TYPES OF DRONES

Fixed-Wing Drones: Drones with fixed wings are characterised by their hard structure and wings, which enable them to fly for extended periods of time at great speeds. They are typically employed in missions involving observation and reconnaissance.

Multirotor Drones: These drones are ideal for tasks requiring hovering or low-speed flight, such aerial photography and surveillance, because they feature many rotors and are very manoeuvrable.

Single-Rotor Helicopter Drones: Drones with a single big rotor and a tail rotor, resembling classic helicopters, are known as single-rotor helicopter drones. They are frequently employed in military and industrial settings and are able to transport larger payloads.

Fixed-Wing Hybrid VTOL Drones: Drones that combine the efficiency and speed of fixed-wing aircraft with the vertical takeoff and landing (VTOL) capabilities of multirotor drones are known as fixed-wing hybrid drones. They work well for mapping and long-range reconnaissance tasks.

Nano Drones: These drones are so tiny and light that they can fit in your palm. They are typically employed in missions involving surveillance and indoor reconnaissance.

Drones Powered by Sunlight: These drones have solar panels installed, which enable them to use the sun's energy to recharge their batteries. They are employed for long-duration missions and have the capacity for longer flight durations.

Delivery Drones: These unmanned aerial vehicles are engineered to transport goods, food, or medical supplies to isolated or challenging-to-reach locations. Businesses like UPS and Amazon are testing them for last-mile delivery.

Combat Drones: Also referred to as unmanned combat aerial vehicles (UCAVs) or armed drones, these drones are outfitted with weaponry for use in combat. They are employed in targeted strikes, reconnaissance, and monitoring.

II. ROLE OF ROBOTS IN WARFARE

Robots are essential to modern combat because they have special qualities that improve military operations' efficacy and security. Below is a summary of their responsibilities, with

references to more reading in the footnotes:

Patrol and Reconnaissance: Robots, such as drones, are widely employed in patrol and reconnaissance operations. They are able to acquire intelligence, track the activities of adversaries, and give commanders real-time situational awareness[1].

Explosive ordnance disposal (EOD) robots are utilised to securely get rid of dangerous chemicals and other improvised explosive devices (IEDs). By enabling soldiers to manage risky circumstances remotely, these robots contribute to their protection.

Logistics and Support: In difficult environments, robots are employed for logistical duties including moving equipment, supplies, and ammunition. They can also be utilised for supply runs to far-off or unreachable locations[2].

Combat Operations: Unmanned ground vehicles (UGVs) equipped with weapons are among the robots built specifically for use in combat situations. By engaging enemy forces, delivering fire support, and carrying out other offensive tasks, these robots lessen the danger to human soldiers.[3]

Medical Support: Wounded soldiers can be safely removed from the battlefield by means of medical robots. They can even help in field hospitals by carrying out simple medical procedures or supplying medical supplies.

Communication and Jamming: Robots can be employed to relay messages and obstruct communications from adversaries. They can interfere with hostile command and control systems and support the upkeep of secure communication links.6

Psychological Warfare: Certain robots, such drones employed for intimidation or propaganda, are made specifically for psychological warfare. These robots have the power to affect the attitudes and actions of opposing forces.

III. SAFE USE OF ROBOTS IN APPLICATIONS

Due to their same foundation, the robotics platform and the standard computer systems platform share many security concerns. The majority of the components that make up robotic platforms are software and hardware. As general-purpose robots gain popularity, numerous applications that let the robots do particular jobs also emerge.

[1] Ronald C. Arkin, "The Role of Robots in Future Warfare," IEEE Transactions on Robotics, 2009.
[2] The Growing Significance of Robotics in Military Operations: Robots on the Battlefield," Centre for a New American Security, by Paul Scharre, 2015.
[3] Strategic Studies Quarterly, "Military Robotics: Latest Trends and Spatial Patterns of Diffusion," Michael E. Miller, 2018.

For this reason, the robot needs to be secured. While system security can be achieved through high-level abstractions, privacy is a significant problem that can be addressed by specific access control techniques. Privacy is guaranteed since people are identified securely and privileges are assigned tiers. Certain software designs have been suggested to guarantee robotic security. Policies for robots are defined by high level abstractions. Web browser security has further implications. System security may be achieved more simply if the framework's major components are divided and a strict interface is defined between them. In this instance, the intercomponent contacts will go via a shared message passing interface that is transparent to the observer. The suggested architecture shown in the illustration looks like a microkernel living in a thin layer of software that is in charge of sending various messages. Robot abstractions, application abstractions, and hardware-specific functionalities are implemented at the aforementioned layers. The abstractions are utilised by the top-running programmes.

IV. CYBER WARFARE

The term "cyber warfare" describes the employment of malicious software, hacking, and other digital attacks to obtain unauthorised access to computer networks, systems, or data, or to disrupt or harm them. This type of warfare takes place online and can be directed on a variety of targets, such as individuals, groups, governments, and the military. Cyberwarfare can be used for sabotage, espionage, and influencing social or political consequences, among other things.

Types of cyber warfare

A variety of techniques and approaches are included in cyberwarfare, with the goal of impairing or harming computer networks and systems. Typical forms of cyberwarfare include the following:

Attacks known as **denial-of-service (DoS):** In these attacks, a target system is overloaded with traffic, rendering it inaccessible to authorised users.

Distributed denial-of-service (DDoS) similar to dos attacks are harder to fight against because they originate from several sources.

Malware is malicious software that aims to infect computers and cause harm or disable them. Ransomware, worms, and viruses are a few examples.

Phishing: When someone impersonates a reliable organisation in an attempt to deceive a user into divulging important information, including credit card numbers or passwords[4].

Information warfare is the practice of using technology to obtain a competitive edge over an adversary, frequently by psychological warfare, deception, or propaganda[5].

Cyber Espionage: Often carried out by nation-states or intelligence services, cyber tools are used to penetrate target systems and obtain intelligence.

Sabotage: Intentional acts intended to interfere with or harm computer networks, systems, or infrastructure, frequently with the intention of causing harm to oneself or financial loss[6].

V. IMPACT ON WARFARE CONFLICT

Robots, cyberwarfare, and drones have all had a big impact on conflict and warfare, changing how battles are fought and tactics are created. The following are some significant effects:

Enhanced Precision: By using sophisticated sensors and targeting systems, drones and robots may carry out accurate attacks on adversary objectives, minimising collateral damage and casualties among civilians.

Decreased Risk to Human Soldiers: By using robots and drones, military forces may carry out risky missions and engage in combat without endangering the lives of their soldiers.

Improved Surveillance and Intelligence Gathering: Drones and robots can collect intelligence in real time, track the movements of adversaries, and give commanders situational awareness, which facilitates better decision-making.

Extended Reach: Robots and drones can enter difficult-to-reach or dangerous-for-human-soldiers' areas.

VI. EFFECT ON MILITARY OPERATION OF ROBOTS DRONE AND YBER WARFARE

Robots and drones provide real-time data and imagery for enhanced intelligence, surveillance, and reconnaissance (ISR)—a process that enhances situational awareness and decision-making.

[4] "Phishing Exposed," by Lance James, Syngress, 2005.
[5] Dorothy E. Denning, "Information Warfare and Security," Addison-Wesley Professional, 1999.
[6] Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to Do About It," Ecco, 2010.

The ability to hack and monitor adversary communications and networks is made possible by cyber capabilities.

Precision and Targeted Strikes: Robots and drones are capable of carrying out targeted strikes on adversary objectives with minimal collateral damage and casualties among civilians. Cyberwarfare may precisely target and disable enemy capabilities by taking down particular systems or infrastructure.

Logistics and Support: By utilising robots for logistics jobs like equipment and supply transportation, the need on human resources can be minimised.

In distant or difficult areas, drones can support medical evacuation efforts and provide supplies.

Force Multiplier: Drones and robots augment human forces' capabilities, enabling them to carry out operations more safely and effectively.

Cyberwarfare can impair the enemy's capacity to respond by interfering with their communications, logistics, and command and control systems.

Asymmetric Advantage: When confronting asymmetric threats like guerrilla or insurgent organisations, militaries can benefit from the use of drones, robots, and cyberwarfare. They make it possible to react to unconventional warfare methods with more agility and adaptability.

Psychological Effect: Adversaries may experience psychological effects from the deployment of drones, robotics, and cyberwarfare that affect their actions and choices. Enemy morale and cohesion might be affected by the threat of being the target of drones or cyberattacks[7].

VII. ETHICAL AND LEGAL CONSIDERATION

Ethical and legal considerations surrounding the use of drones, robots, and cyber warfare in military operations are complex and have sparked debate among policymakers, scholars, and the public. Here are some key points:

Civilian Casualties: One of the primary ethical concerns is the potential for drones, robots, and cyber-attacks to cause civilian casualties. The precision of these technologies can reduce collateral damage compared to traditional warfare, but the risk remains.

[7] "The Psychological Impact of Drones on the Communities of Pakistan and Afghanistan," by Ayman Sawaf, Journal of Strategic Security, 2013

Targeted Killings: The use of drones for targeted killings, especially outside of traditional battlefields, raises questions about due process, sovereignty, and the legality of extrajudicial executions[8].

Autonomous Weapons: The development of autonomous drones and robots capable of selecting and engaging targets without human intervention raises ethical questions about accountability, control, and the risk of unintended consequences.

Privacy: Drones and cyber surveillance raise concerns about privacy rights, as they can be used for mass surveillance and data collection without consent.

Cyber Attacks and Proportionality: Cyber-attacks can have far-reaching consequences, including civilian infrastructure and essential services. Ensuring that cyber-attacks are proportionate to the military objective is a key ethical consideration.

Attribution and Accountability: One of the challenges of cyber warfare is attributing attacks to specific actors, which can complicate efforts to hold perpetrators accountable under international law.

International Law: The use of drones, robots, and cyber warfare is governed by international humanitarian law, including the principles of distinction, proportionality, and military necessity. Adhering to these principles is essential to avoid violations of international law.

Human Rights: The use of drones, robots, and cyber warfare can impact human rights, including the right to life, freedom from torture, and privacy. Ensuring that these technologies are used in accordance with human rights standards is a key ethical consideration.

Transparency and Oversight: Ensuring transparency and oversight in the development and use of drones, robots, and cyber warfare technologies is essential to address ethical concerns and maintain public trust.

VIII. CONCLUSION

In conclusion, the use of robots, drones, and cyberwarfare in military operations has changed the character of conflict and presented new difficulties for contemporary armies. These technologies have lowered hazards to human soldiers and improved targeting accuracy and efficacy as well as intelligence, surveillance, and reconnaissance capabilities. However, its use presents moral and legal questions about things like privacy rights, autonomous weaponry, targeted murders, and civilian casualties.

It is necessary to carefully analyse human rights concepts, international humanitarian law, and ethical standards in order to address these concerns. In order to guarantee that these technologies are used responsibly and in compliance with existing legal frameworks, transparency, accountability, and supervision are crucial. It is critical that decision-makers, military chiefs, and the general public have educated conversations as technology develops.