International Journal of Engineering& Scientific Research
Vol.13 Issue 07, July 2025
ISSN: 2347-6532 Impact Factor: 8.076
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

A Thematic Paper on Information Warfare: It's Omnipotence and Impact in War

Col Diganta Choudhury (retired)

Abstract

Information Warfare (IW) is the warfare of Information Age. In recent years, with Information and Communications Technology (ICT) covering newer thresholds, the role of 'information' in warfare has evolved radically into a heterogenous phenomenon concerning deployment of weapon systems and cyber warfare. Equally, history is replete with examples of technological breakthroughs, resulting in cascading changes affecting the very structure of civil society and military organizations. Such changes also impact IW, which, when conducted through a technique of information *disturbance, degradation* and *denial*, becomes more innovative and deadlier.

IW has no specific frontline and no geographical boundaries. It is relatively low cost, highly effective and is redefining the concept of warfare. Ethical and legal boundaries are stretched thin by IW and all its manifestations. As IW is all pervasive, the ethical rights of individual liberty, privacy and anonymity will be breached. There is also a potential risk in increase in number of conflicts and casualties. It is critically important, therefore, to *understand* all its nuances of IW and *prepare* for it. As evinced from Russo-Ukraine war and the Israel-Hamas conflict, unless doctrines have evolved, strategies are in place and battle space prepared, nations will be left defeated by onslaught of IW.

India faces hostile neighbors who have used cyber space and psychological warfare to spread disinformation and disruption internally, besides the existing external threat. It must learn therefore, to control its information space, protect access to own information, while acquiring and using the adversary's information, as well as disrupting their flow of information. Technological advancements must be dovetailed into the system to stay ahead of the curve.

INFORMATION WARFARE: IT'S OMNIPOTENCE AND IMPACT IN WAR

The concept of Information Warfare is as old as warfare itself. Sun Tzu, in **The Art of War** (515 BCE), his poetic and potent treatise on strategy, states that *warfare is the way of deception. Thus, although capable, display incapability to them. When committed to employing your forces, feign inactivity. When (your objective) is nearby, make it appear as if distant.* History is replete with examples of various forms of Information Warfare with all its various facets.

Definition

Information Warfare (IW) is an operation conducted to gain information advantage over the opponent, to achieve strategic goals.It consists of controlling one's own information space, protecting access to one's information, while acquiring and using the opponent's information, destroying their information systems and disrupting their information flow.

IW may also be defined as actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and protecting our own information and systems.

A Historical Perspective

Sun Tzu's treatise was the *first documented* codification of use of intelligence and psychological operations to achieve strategic or operational goals. He stated that to win hundred victories and to subdue the enemy *without* fighting is the acme of skill. Alvin Toffler in his seminal books *The Third Wave* and *War and Anti War* (with Heidi Toffler), describe a future environment in which we will have to act and react to the impact of information revolution, the onset of the postulated third wave and its impact on future warfare.

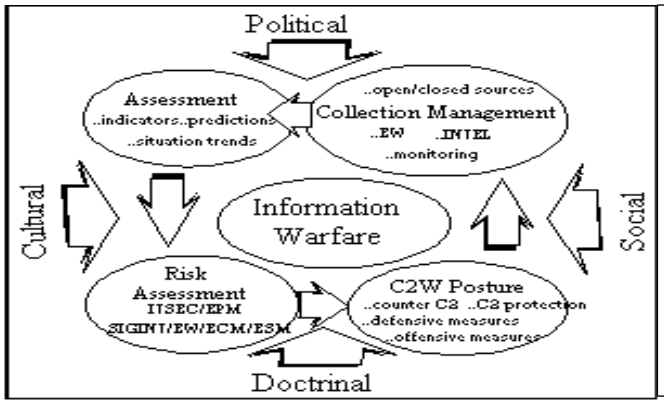
Genghis Khan (1162-1227) successfully conquered large parts of Central Asia and China by spreading deceit, misinformation amongst his rivals, allied with his strong intelligence mechanisms. During the 1750s, Frederick the Great employed long term intelligence system for information gathering and incorporated spy networks. IW has evolved over time and technology. The French Army, during World War I, conducted IW activities using electronic warfare technology that enabled interception of wireless and telephone communication. During *Operation Fortitude* based in Dover, United Kingdom, military deception of massive scale was carried out wherein a fake First US Army Group (the Ghost Army), led by George Patton produced fictitious radio traffic, displays and false media coverage. The German Western Front defenders remained rooted to Pas-de-Calais (France), expecting the invasion there, even as it unfolded in Normandy. The recent Russia-Ukraine and the Israel-Iran conflict reinforces the IW omnipotence.

Emergence of Information Warfare

Information about own and enemy forces, terrain, intention of adversary etc, has always been an important part of national security and essential for successful conduct of war. Dramatic advancement in fields of Information and Communication Technology has paved the way for a whole new range of weapon systems and refined military doctrines. Hence, information superiority over the adversary is of paramount importance in war.

Figure 1: Gamut of Information Warfare

Areas of Information Warfare Technology



Political: Economic antagonism, political tension, power inequality.
Social: Clash of social interests and classes.
Doctrinal: Manipulating public, control information space, shape perceptions.
Cultural: Community involvement and education, organisation landscapes.

Doctrines of IW have evolved, and current ones envisage *continuous domination* of the information sphere across full range of operational spectrum, as well as complete battlefield transparency and real time situational awareness at all levels of command. In order to support this doctrine, the force capabilities should include the following:

- Should be able to optimize information-based operations.
- Dominate battlefield with speed, space and time.
- Ability to control the battlefield with lethality and superior survivability.

- Be capable of quick and decisive victories with minimum casualties.
- Be effective in war (and operations other than war, ie, counter insurgency/ terrorist operations) as part of joint team in all operational environments.

Given the force capabilities elucidated, it would be prudent to examine all the facets of IW and how it impacts the joint war fighting.

Information Warfare through Electronic Warfare

Electronic Warfare represents the ability to use electromagnetic spectrum to secure and

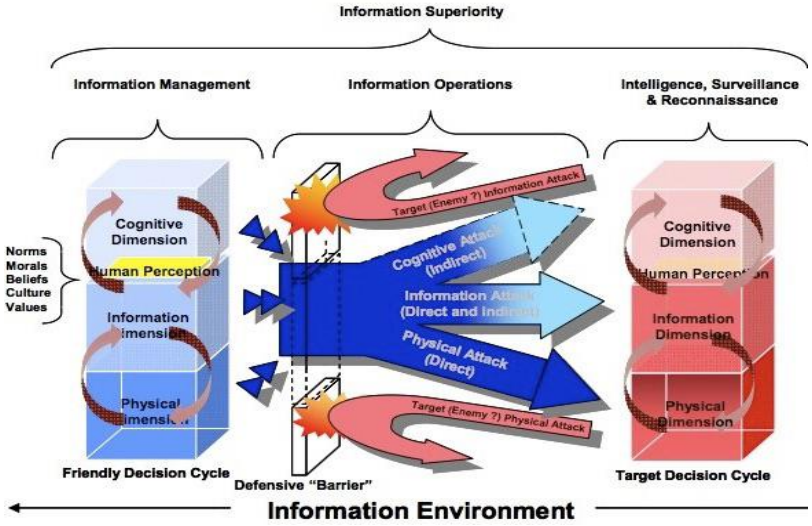
Electronic Warfare:
Cyber Electronic Warfare
Electromagnetic Deception
Airborne Electronic Warfare
Electronic Security
Infrared & radio frequency countermeasures
Electronic Probing
Electromagnetic Interference/pulse

Figure 2: Electronic Warfare

Maintain effective control over the spectrum, attack the enemy or impede enemy assaults. Equally, Electronic Warfare can disrupt, deny and degrade adversary's ability to use these signals. Awareness and surveillance, protection and denial of information are the keys to dominating the electromagnetic spectrum. Electronic Warfare can be applied from air, sea, land and space, by manned and unmanned systems.

Information Warfare through Cyber Warfare

Actions by nation states or international organizations from computers and networks connecting them, against government and military network, to *disrupt*, *deny* or *destroy* their use are referred to as cyber warfare. Cyber warfare reportedly began in 2010, with the use of a computer worm called *Stuxnet*, which destroyed 20% of the centrifuges used by Iran to create nuclear weapons (**Circa:June 2025** bombing of Iran's nuclear installations). Cyber war activities may consist of hacking information system, as China did by stealing federal



employee information in US in 2015. It may also involve 'social cyber attacks', by creating a specific image consistent with the goals of IW. Social network sites are also valuable sources of information on the target group to which (dis)information activities are to be addressed. IW over the internet uses amongst others, *troll factories* (entities employing people who post comments on the net), *bots* (programs sending out periodic messages) and *fake news* etc.

Figure 3: Depicts the Information Environment and its Management

Resorting to cyber warfare by attacking and defending information and computer network in cyberspace, while denying the adversary's ability to do the same is very essential to gain ascendency. This can be achieved through *attacking* the adversary's information (stealing information), their information-based processes and networking, information and communication system and *defending* own systems and processes.

Resorting to cyber warfare as part of IW has its own challenges. Ipso facto, there are no physical boundaries, no front line and no physical battlefield in a cyber warfare environment. Entities, persons and organizations carrying out cyber warfare is difficult to detect. Given these characteristics, waging of cyber warfare as part of IW to achieve overall objectives will be the *warfare* of the future.

Cyber Enabled Information Warfare and Information Operations

Application of cyber enabled information operations in the IW doctrine is very highly technology based. Such technology on which a force will depend, is composed of:

- Command,Control,Communication,Computation and Intelligence (C4I).
- Intelligence, Surveillance and Reconnaissance (ISR).

The C4I system must include the aspect of interoperability that alone can ensure a synergistic application of various components. Modern communications are an extensions of computer networks through switching and media technology; hence the fourth 'C' in C4I system may denote coordination.

Lockheed Martin uses C4ISR technology 'to turn abstract data into operational decidedness'.The C4ISR technologies enable accomplishment of diverse set of missions in air, sea, land and space. The operators gain decision advantage from a command-and-control system that allows for parallel (not sequential) planning and decision-making abilities. These systems enhance situational awareness and therefore, stay ahead of adversary in an accelerated operational environment.

Information Dominance — Battlefield Awareness — Decision Advantage

ISR functions in combat zone are done through *surveillance* (looking for data in the battlefield), *reconnaissance* (specific search for information and data) and *intelligence gathering* (by automated processing, fusion and correlation to support or negating a decision). Across air, land, sea and space, sensors on board, manned and unmanned military platforms etc, are collecting huge data. These ISR systems task, collect, process, analyse, fuse and disseminate most mission critical information. For better information fusion and data analytic, the system must support decision advantage by performing advance

correlation, fusion and analytic across multiple domains and class levels. Efficient command, control and battle management system requires innovative, cost efficient, airborne and ground system configuration that address a wide range of intelligence, surveillance and reconnaissance requirements.

Information Warfare through Psychological Warfare

There has been a growing debate in military circles regarding the asymmetrical threat and latent possibilities of IW, both offensive and defensive, vis-à-vis Psychological Warfare. It is imperative therefore, to critically examine the latent role of psychological operations in IW and its future strategic impact as well as the operational capabilities required to meet that role.

Psychological operation is a critical element in affecting the will of the adversary to fight. There are innumerable examples of successful application of psychological operations in support of deception operations or in direct support of the goals and objectives of the force, conducted well before and during military operations. Chinese military strategy categorizes psychological operations as *offensive and defensive combat action that uses specific information and media to influence the psychology and behavior of the target object through rational propaganda, deterrence and emotional guidance based on strategic intentions and combat missions.* Non state actors and armed groups also conduct psychological operations. Hassan Nasrallah, the leader of Hezbollah (killed on 24 September 2024), had postulated that the *most advanced and important weapon is psychological warfare.*

Psychological warfare as an integral part of IW is carried out by the employment of communication and other means to influence the views, attitudes or behavior of the adversary or civil population towards military or political objectives. Towards this aim, India's counter insurgency doctrine is amalgamated with successful application of psychological operations to achieve operational or strategic goals. Need of the hour is a 'Psychological Operations Task Force' with adequate structure, force and resources, amalgamating all the relevant stakeholders for successful conduct of IW through own psychological operations and influencing the behavior of the target population.

Information Warfare and Military Deception

Trojan Horse, which led to the Greek seizure of seemingly impregnable fortress of Troy, is one of the earliest examples of (military) deception as a means to win the war. Actions taken to mislead opponent decision makers into taking specific actions (or lack of actions), that contributes to the success of one's own effort, is a timeless aspect of military deception and IW.

Paradoxically, in an era of information saturation, deception in warfare is more difficult to achieve and most critical to operational success. Military deception is often neglected or discounted in planning phase. At times, it is also developed in a compartmentalized manner, rather than a deliberate part of the overall objective. Military deception is not only the key and integral aspect of successful operation, but it also has the potential to change the course of war. Military deception is highly sought and emphasized by India's adversary, China. It needs to be understood that the PLA espouses military deception in totality, placing it amongst their key fundamental principles for successful operations. Ipso facto, India stands to gain by incorporating military deception in its operational doctrine. While there is an apparent risk of faulty deception operations in IW, there are greater opportunities of

achieving surprise, indecision and stagnation amongst the adversary, which can be swiftly exploited to achieve complete superiority.

Information Warfare and Operational Security

Operational Security can be best defined as the security and risk management process that prevents sensitive and confidential information from falling into the adversary's hand which can be exploited to their advantage. There is no gainsaying the fact that any breach in operational security will critically harm the military plan or objectives and therefore, all efforts must be incorporated in planning and execution of operational security as part of IW. The following processes make up operational security:

- Identification of critical information.
- Analyze the threats, vulnerabilities and risks that exists.
- Apply appropriate countermeasures to deny any breach of critical information.

IW uses critical information systems and electronics to gain material advantage in operations.Therefore, these systems and processes are to be used as countervailing measures. The process includes the following:

- Disinformation – spreading fake news or information.
- Disruption – Jamming and hijacking.
- Exploitation – Use of social media and online platforms to create suitable narrative and manage perception.
- Cyber Attack – Exploiting weak information security.

Therefore, it is of critical importance that the security and risk management process that prevent sensitive information getting into the hands of the adversary, must be made foolproof. Any innocuous act that could reveal the hand must be streamlined to prevent leakage.

Information Warfare and the Changing Face of War

With the coming of age of IW, the traditional concept of warfare has undergone a sea change. In fact, there has been a blurring of geographical boundaries. War is no longer fought by militaries only, with state and non-state actors proliferating and profiteering from IW, especially in cyber domain. The aspect of risk to infrastructure

Advances in Technology: Evolution of cyberspace, microcomputers, info technologies etc has *revolutionised* warfare.
IW: Using communications, diplomacy, information to gain political and military ascendency. Allied with artificial language, it enhances cyber, physical and biological attacks. Hybrid warfare is the order of the day.
Military Doctrine: Military strategy and doctrine have evolved manifold.

Figure 4: The Changing Face of Warfare

Is more heightened than ever before. New information-based technology has come to fruition, thereby increasing the power of deception and manipulation at multiple levels. New strategies and doctrines have come to fore and dovetailed in planning and execution level with the rapidly evolving IW being at the centre stage.

Equally, the role of the Government has become more intense, all-encompassing as it organizes, equips, trains and sustains military forces and lays down policy and directives.

With incorporation of many evolving facets in IW, the authorities have to play a more productive and efficient role as facilitator and maintenance of certain information systems and infrastructure to reduce vulnerabilities. It also may need to facilitate and manage public perceptions and loss of certain civil liberties amongst the civilians as a result of the all-pervading IW.

Future of Information Warfare in an AI Powered World

Artificial Intelligence (AI) has changed our everyday lives in innumerable ways. But how revolutionary will AI be in an IW scenario? If we go by the maxim that IW is the future of warfare, as all the indications point in that direction, then a future warfare with heightened and more developed AI will really change and maneuver, virtually or otherwise, the whole concept and doctrines of IW.

It remains to be seen if AI will make IW and conflict more lethal and equally difficult to constrain. But all indicators point towards that direction. We need to plan for a future in which machines can pilot fighter aircraft more skillfully than humans, AI enabled cyber-attacks devastate enemy networks and an advanced algorithm turbocharge speed of decisions. That AI will significantly change IW in near future is undeniable. However, it will also be prudent to imagine that while regimes will aggressively utilize AI in all facets of IW, the most critical decisions will be kept in human hands. However, AI enabled intelligence and analytical tools can help humans to sift through confusing and fragmentary information regarding the adversary's preparation of war. It is believed that AI helped US intelligence analysts sniff out Russian President Putin's invasion of Ukraine in 2022. Notwithstanding the same, the following domains will reflect the change/upheaval in the IW milieu, in an AI powered world:

- **New Technology**: Introduction of high-altitude Electro Magnetic Pulse (EMP) could disable communication networks and jam satellites.The High Altitude Active Auroral Research Program-me (HAARP), a University of Alaska Fairbanks programming, if weaponized, could unravel radio communication and surveillance in a big way.
- **Space Technology**: Development in drones, satellite technology, antisatellite technology, hypersonic technology are all disruptive and will significantly alter whole gamut of IW.
- **AI, Nanotechnology and Robotics**: Conflict of future could be replaced with robots, capable of taking independent missions. Development in AI has given capabilities in unmanned offensive weapon system, remote attack capability etc. Battlefield has become much more transparent with AI and neural based equipments.
- **Cyber Space**: In the cyber space, smaller nation states are capable of taking on technologically advanced nations. The Stuxnet and Flame attack against Iran and Estonia respectively reflects the power of this maxim. Focus has now shifted from conventional to the virtual domain.

Impact of Information Warfare on National Security

IW at national and strategic levels, fought with complete reach and intensity, can have a catastrophic effect on a nation. By use of *offensive* IW, adversary's C4I can be greatly

disrupted, and its information system can be crippled with a view to create information gaps. Utilized effectively, cyber warfare can manipulate democratic processes, eroding public trust in government. Attacks on military networks, civilian critical infrastructure and communication system are all in the realm of IW. It can also alter public perception which itself can have a cascading effect on the adversary's will to fight a hybrid battle. At the same time, by utilizing *defensive* IW, a nation will seek to *preserve* own critical information and communication system being jeopardized.

It would be therefore, logical to surmise that any information-based society is largely at risk of being *disrupted by* offensive IW. The level of disruption would vary depending on the threat perception and the quantum and ability of own defensive IW to negate such attack. National security, inextricably linked to these information-based systems and infrastructure, would invariably be affected and severely impacted. These information-based systems include complex management systems and infrastructure involving control of money flow, logistics, traffic and are prone to increased vulnerabilities. Computers from multiple locations with multiple link infrastructure are also vulnerable to psychological operations, C4ISR, electronic warfare etc, thereby impacting national security. As a nation, it is of critical importance therefore, that own defensive IW be securely incorporated in place.

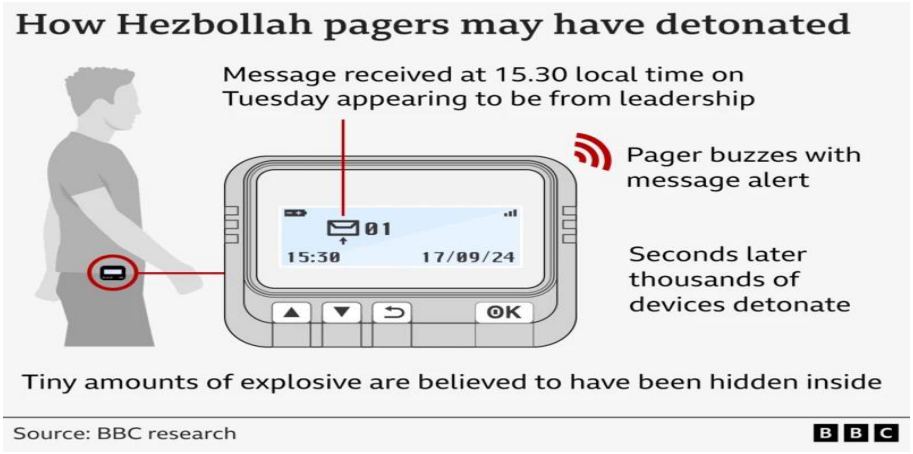
Information Warfare: A Philosophical Perspective

It is said that the information revolution is the *fourth* revolution after the Darwinian, Copernican and Freudian. As IW is a *byproduct* of information revolution due to a shift to nonphysical domain, it appears to be the way war will be fought in future. IW is reshaping the very concept of warfare, as disruptive, bloodless, cost effective and not military specific operation, with negligible physical commitment. IW does not require military specific skills and technology wherein skilled civilians are competent to wage battle. Metaphorically, it is an important consequence of the contemporary society and the often-blurring distinction between military organization and civil society.IW includes physical and nonphysical warfare. An example is of *Stuxnet*, a computer worm that targets systems not on the internet, but in the industrial networks. It is a good example of environmental transversality as it is a digital, nonphysical weapon, able to affect and disrupt objects in the physical domain.

Ethical, Legal, Political and Social Issues Relating to IW

It is evident that IW is redefining how war is waged. In doing so, it is reshaping the very concept of war itself by raising new ethical issues and challenging old dogmas. J Robert Oppenheimer, the American theoretical physicist (and Director of *Project Manhattan*) had opined that, 'war is a contention between two or more states through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases'(*Lauterpacht, 1952*). Such concepts of war waging have undergone a radical shift due to coming of age of IW, which is all pervasive. Therefore, the ethical rights of individual liberty, privacy and anonymity may be subverted. There are also concerns about moral and legal ambiguities regarding the aspect of *traceability* of initiator of cyber-attack. In a recent case of 17/18 September 2024, thousands of pagers and radio devices exploded in Lebanon, killing at least 37 people and injuring thousands (*BBC News*), raising more ethical, legal and political issues then there are answers.

Figure 5 below: Depicts how pagers and devices may have detonated



(**BBC)**

It is evident that civilian technology can be targeted or attacks from civilian technology can be carried out, which is difficult to control. IW, therefore, reflects a staggering revolution which may concern military affairs, but has political and social ramifications for society as well. It is evident therefore, that there is a huge vacuum in ethical principles and regulations and in the coming years, this chasm is only likely to grow.

IW in Russia-Ukraine War:Lessons For India

On 24 February 2022, Russia invaded Ukraine in a major escalation of the Russo- Ukraine war, which started in 2014. Since then, there has been an explosion of IW strategies by both the warring nations and NATO.

- **Russia**: IW strategized to justify Ukraine invasion, destabilize Ukrainian army/ government and put blame on capitalists. Equally, mobilize the Russian public opinion to support Kremlin and *limit* flow of external information into Russia. IW is integrated into Russian thinking on war, run by security agencies, media and the *grey zone actors, ie, Internet Research Agency*.
- **Ukraine**: Sow discord amongst Russian people, convince Russian soldiers to surrender and publish their death tolls. Internally, they strengthen control over media, created Information security awareness amongst own people and secure a positive image in West, to gain moral support and weapon systems.

An important lesson for India from the Russo-Ukraine IW is that all liberal democracies face tremendous hurdles in their struggles in limiting IW from the adversary and it also affects own discourse. There is, therefore, an immediate requirement of distinguishing between authentic discourses and the *views* planted. Designated civil entities must be established to work with civilian agencies to debunk disinformation campaigns. It is equally imperative that civil society be suitably organized to take action to raise public awareness on this important issue, within the State's overall framework.

Epilogue:IW in Modern Political Theory and Lessons For India

Political theorization of IW encapsulates the entire gamut of history as well as analyzing the relationship between the polity, the Government and the labyrinth of IW that we see today, given the geopolitical situation worldwide and specifically the threat perception in India.The

information dimension or aspect of warfare is increasingly becoming central to outcome of battle and therefore, need to be addressed accordingly.

India faces a hostile neighbor in its north and as has been evident so far, China has used the information dimension to its strategic advantage. People's Liberation Army (PLA) believes that no matter the type of warfare or military activity, the *foundation* of it remains IW. PLA will attack the adversary's operational systems, the operational architecture and try to *slow down* enemy systems in a temporal sense.

Against this backdrop, it is imperative that the government must be *equipped* to fight this strategic information battle. A joint doctrine for information-psychological operations covering concepts and information modalities as well as interplay between them has to be promulgated. Army specific doctrine must also be on anvil. Five-dimensional battle space with Information space (as opposed to cyber space) must be endorsed in the doctrine. It is of critical importance to endorse the *reality* that conflict in this virtual and artificial dimension is *at par* with traditional notion of warfare in physical realm, in so far as devastation and destruction is concerned. There is also no gainsaying the fact that for carrying our offensive cyber operations, raising of a cyber command is a strategic necessity, with cyber units at tactical level to execute such operations.

References

I. Aro, J, "The Cyber Space Warfare: Propaganda and Trolling as Warfare Tools", (2016).
II. China National Defense Strategy, "Science of Military Strategy", (2020, Chapter 11, Section 10).
III. Defense Technology Information Centre, "National Security and Information Warfare", URL: https://apps.detective.mil.
IV. Defense Technology Information Centre, "Information Warfare".
V. Simon Ewing-Jarvie, "Information Environment", URL: https://defsec.net.nz.
VI. Floridi, L, "The Ethics of Information Warfare".
VII. Hertfordshire University Research, "Information Warfare Philosophy", URL: https://researchprofiles.herts.ac.uk.
VIII. Mitnick, Kevin, "The Art of Invisibility", (Little, Brown and Company, 2017).
IX. Molander and Wilson,"Strategic Information Warfare-A New Face of Warfare".
X. NATO Homepage, "A Global Information Certification Paper",URL: https://nato.int.
XI. Ohlin and Finkelsteen, Oxford University Paper on Cyber Warfare, "Law and Ethics of Virtual Conflict", URL: https://academic.oup.com.
XII. Pakistan Defense Paper, "Indian Non-Contact Warfare".
XIII. Rudi, Rudolf, "Doctrine on World of Information Warfare".
XIV. Toffler, Alvin, "The Third Wave", (William Morrow, 1980).
XV. Toffler, Alvin and Heidi, "War and Anti-War", (1993).
XVI. United States News, "International Law Studies", URL: https://common.usnewsc.edu.
XVII. Vivekananda International Foundation, "Cyber EnabledInformation Warfare", URL: https://www.vifindia.org.
XVIII. Vivekananda International Foundation, "Changing Dimension of Information Warfare".