NDC JOURNAL
Security Through Knowledge

IMPACT OF INFORMATION REVOLUTION ON STATE SECURITY

Brigadier Basit Raza, ndc, afwc, psc, MCILT (UK)

"There is a war out there, old friend, a World War. And it's not about whose got the most bullets; it's about who controls the information: what we see and hear, how we work, what we think. It's all about the information."

-Cosmo

INTRODUCTION

"Information Revolution" as a phenomenon cannot be simply portrayed. It was originated by the invention of printing press and had been reinforced all along with the inventions of radio, telephone and television etc. However, it became truly a revolution with introduction of Information Technology (IT). While information revolution has innumerable features; ***complexity and change are its central characteristics***. ***Its challenges thus also lie in its complexity and speed of change***. Today, the success of organisation, societies and states depend upon their abilities to adapt to intricate challenges and exciting opportunities afforded by the advent of Information Age. State security as an emerging paradigm for understanding global opportunities and vulnerabilities is strongly linked to information revolution. Information boom has enabled states to equip themselves with the power of knowledge and thus should not be dependent upon inheritance to make a place in the world. Moreover, these impacts are not confined to state only, rather transcend down to organisation, institutions and society. On the other hand, the accelerated pace of globalization has affected the distribution of power between state and non-sate actors as the power of non-state actors has been growing within the interstate community. These changes have substantial impact on the power and security of the state.

The interstate networking of system has created synergy with great dividends to countries; apart a substantial impact on the power and security of the state. Thus, realizing the strategic importance of intelligence and information ranging from political, economic, and military to cyber ones, resultantly the states have increased their focus on gaining intelligence-related information and deny it to the potential enemies through Information and Intelligence Wars. Moreover, the workings of terrorist organisation have made the intelligence work more sensitive and the state patronage to non-state actors in the field of intelligence-information has gone much forward. The arena of Information and Intelligence Warfare is taking totally new turns in context of extremist forces; jumping intelligence the warfare by the employment of modern IT. As a consequence, the warfare has expanded to the level of the blurring of civilian and military lines, with heightened vulnerabilities of social, political and even cultural centres of gravity, signalling alarm bells for all round security of states in 21st century.

Today, nations cannot avoid confronting various global issues in this age of information revolution. By remaining as a closed society, no country can prosper in present world; which has become globalized because of rapid advancements in IT. Therefore, this revolution has a direct impact on the states security. Due to positive governmental policies worldwide in last decade or so the scientists and engineers have made greater strides in the sphere of IT as compared to twenty years back in the history. Intelligence connectivity, private television channels, FM radio stations and cellular phone services have seen an exponential rise in this time period. All these have impacted states security in multiple ways by throwing daunting challenges and also proving exciting opportunities.

Fundamentals and Conceptual Parameters of Information Revolution

Basic Terminologies. It is deemed necessary to define information notion and its attendant terms to assess multi-dimensional impact of information revolution.

Information. Webster defines that "information is meaningful; it has subject; it is intelligence or instruction about something or someone". The other definition is provided by denoting; "whatever can be coded for communication through a channel that connects a source with a receiver".

Revolution. A revolution is a fundamental change in power or organizational structures that takes place in a relatively short period of time and their results include major changes in culture, economy, and socio-political institutions. It is also defined as "primary change in the way of thinking or visualizing something; a change of paradigm especially in technology; under taken in a comparatively short period of time.

Information Revolution. In general terms information revolution describes existing economic, social and technological trends beyond the industrial revolution. The information revolution is also defined as "proliferation of availability of information and accompanying changes in its storage and dissemination owing to the use of computers, internet and other electronic devices".

Information System. "Information System" is the one which handles information, and may include any or all of processing, storage or communication. A computer based information system uses computer technology to process raw data into meaningful information. It is technically a set of interrelated components that collects, retrieves, processes, stores and distributes information. A communication system is a form of information system.

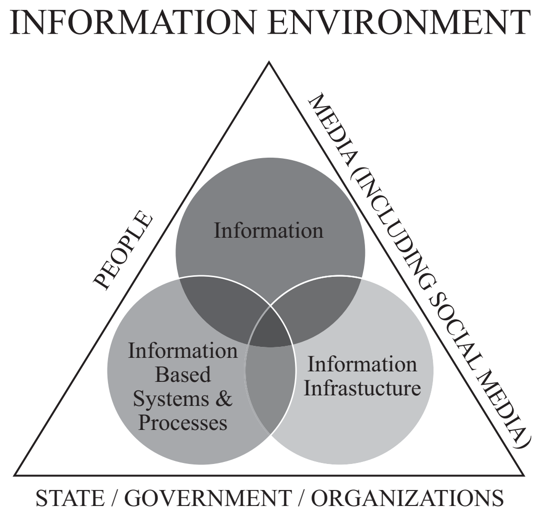
Notion of Information Revolution. Information revolution is third in line of great civilizational revolutions preceded by Agricultural and Industrial revolutions. These initial revolutions were *slow and localised in nature but information revolution by nature* *of its vary mediums has been a lot faster and global in reach*. As industrialism was marked by mass production, informationalism is *characterized by flexible production;* resultantly, it becomes the single most important force shaping communities today.

Interplay of Information Taxonomy

Global Information Infrastructure. Global information infrastructure is combination of convergence of ITs, communications, information and people. This architecture forms a global community, which is networked and interlinked through multiple communication means. Information is generated and shared in virtual time.

Information Environment. Basic paradigm of the information is information environment (Figure-1), which determines the different parameters of the very concept and how it is utilized or attacked. Information environment essentially includes information, information infrastructure and information based system and processes. Stakeholders in this triad are the states, governments, organisations, media (including social media) and people/general public.

Figure 1: Info Environment


INFORMATION ENVIRONMENT
PEOPLE
MEDIA (INCLUDING SOCIAL MEDIA)
Information
Information Based Systems & Processes
Information Infrastucture
STATE / GOVERNMENT / ORGANIZATIONS

Role of IT in Information Revolution

Impact of Technologies. The advancements have impacted IT; which in turn has caused information revolution. The impacts of technologies are as under:-

Enhanced Speed. The speed with which information can be transmitted, manipulated and interpreted has increased significantly and will continue to increase. This enhanced speed of surge of information has an imprinting effect on the frequency of interactions.

Larger Capacity. The ability to transmit information has increased considerably with enhanced capability to interpret vast stretch of information concurrently. It allows decision makers to have access to greater picture of the world, which facilitates their decision making process.

Greater Access. Technological advancements have provided greater information access and opportunities to people and organisations. It leads to "democratisation" of information and global reach to communication flow. It further causes decrease in hegemony of few government, businesses and organisations to dominate information and communication links.

Global Connectivity. Development in communication made it possible to send voice data and picture messages across the globe thus, developing the concept of "Global Connectivity" in earlier timeframe.

Information Revolution and State Security

Notion of State. A state can be defined as " *a community of persons more or less numerous, permanently occupying a definite portion of territory, having a government of their own to which the great body of inhabitants render obedience, and enjoying freedom from external control*". Its notions of territorial occupation and freedom from external control have been challenged by the onslaught of information revolution. Moreover, it has also impacted attended notions of state i.e. authority and governance.

Concept of State Security. "State security is the required to maintain the survival of the state through use of economic diplomacy, power projection and political power". Moreover, state security is an appropriate and aggressive blend of political resilience and maturity, human resources, economic structure and capacity, technological competence and availability of natural resources and finally the military might.

Information Revolution and State Security. Information revolution has greatly changed the concept of security in the 21st century. The dependence on IT has made state and institutions highly susceptible to computer interruptions by hackers and undetected insiders or cyber terrorists. Therefore, key state security dilemma of information revolution remains centred on creating effective and transparent government, which should be able to protect its citizens and vital state interests.

Empowerment of Non-State Actors. Empowerment of non-state actors due to information revolution has changed the dynamics of distribution of political power amongst various businesses at social and political levels. The empowerment of non-state actors comes at the expense of power of the state. These new non-state actors include trans-state corporate organisations, special groups, NGOs and terrorist organisation etc.

Challenges by Information Revolution. The salient challenges posed by information revolution to state security are as follow:

a. Since developments make communication of information easy accordingly, differentiation within and between states and inter-state actors has become porous and hazy. Despite adding domestic element in state security, vagueness of the domestic-interstate dichotomy has increased, where it is difficult to disconnect state security issues from law enforcement, policing and related concerns. Consequently, such increase in the issues has state security implications; needing attention at all related tiers.

b. Since information revolution has become persistent accordingly, state vulnerabilities are induced with multiplying effect by modification of information, interruption of technologies and loss of control or access to information at the state level.

Vulnerabilities of Free Flow of Information. Free flow of information around the globe through use of internet has raised information security dilemma for maintaining state security. Following main aspects are high-lighted as follow:

a. System commotion through e-assault on stability remains a state security apprehension. Thus, increase in electronic related issues can fall under the domain of state security in contemporary information age.

b. Information revolution takes strength from technological advances and has increased ability to collect enormous quantities of data for conversion into comprehensible information. Subsequently, it transmits the gathered intelligence to decision makers for timely action. Thus, this revolution impacts significantly on means of warfare for attainment of objectives.

c. Recognized interstate actors i.e. multistate corporations and NGOs can follow own goals; which may confront state security, owing to their technological expertise facilitated by information revolution.

CYBER WARFARE AND CYBER SECURITY NEW DOMAINS OF STATE SECURITY

Understanding Cyber Warfare and Cyber Security

Cyber Warfare. Cyber warfare is defined as *"Non-kinetic, offensive actions taken to achieve information superiority by affecting enemy information based processes, information system and computer-based networks"*. It has often been referred to as the 5th domain of warfare.

Relationship - Cyber Security, Information Revolution and Technology. The cyber security debate originated in US in the mid 1990s from where it subsequently spread to other countries and manifested itself on security policy agendas. The subject is a product of two recent developments i.e. information revolution, and the integration of technologies into a multi-media system of communication with global reach. The rise of cyber threats can be seen as major re-orientation of security policies that took place after the end of the Cold War. Observers of technologies trends talk of a "*digital revolutions*" with a massive online activity and social networking. The 21st century networked world has started to recognize the impact of cyber space, its nature and scale of risks that increased dependency has brought. Many of these risks are hidden from plain sight, until they strike.

Conceptual Framework of Cyber Warfare. In "Cyber Warfare" all related terms like software war, hackers' war and cyber attacks converge at one point becomes synonymous to each other. The tools, techniques, actors and even the philosophy are seemingly same. Dominant feature, however, remains the use of cyber space as a medium to wage war and cause massive disruption. Cyber attacks can be launched by terrorists, criminals or by nation states; who cannot afford to wage war against adversaries through conventional means. These elements not only target the web sites of government, armed forces and private companies, but also attack high value targets such as the networks that control crucial infrastructures and installations of strategic values.

Cyber Security. UK's Cyber Security Strategy - June 2009, describes cyber security as *"Citizens, business and government…enjoy [ing] the full benefits of a safe, secure and resilient cyber space and ...seiz[ing] opportunities in cyber space to enhance the country's overall security and resilience*".

Spectrum of Cyber Security

Types of Cyber Attacks. Conceptually, every cyber system consists of four types of components i.e. physical system, transmission system, software and data. Each component is critical to the functioning of the system and is potentially vulnerable to either corruption or disruption. Main types of cyber attacks on each component are as under:

Serial	System Component	Purpose of Cyber Attack	Types of Cyber Attacks
a.	Physical Component	Disable or corrupt computer hardware	Pre-positioned hardware logic bombs, disruption of power supply etc
b.	Transmission System	Intercept or disrupt communications	Tapping, spoofing, overloading, jamming, computer intrusion etc
c.	Software	Disable, corrupt or establish control of software functions	Pre-positioned software logic bombs, exploitation of bugs, viruses, computer intrusion etc
d.	Data	Destroy, steal or corrupt data	Viruses, computer intrusion etc

Major Cyber Attacks of Contemporary Times

Military Domain

US Department of Defence (DoD) and CENTCOM – November 2008. Classified networks at DoD and CENTCOM were hacked by unknown foreign intruders. It took several days to dislodge the intruders and rescue the network .

Stuxnet – 2010. This complex malware was detected in Iran, Indonesia and elsewhere. It was designed to interfere with Siemens Industrial Control System. It is regarded to be a cyber weapon aimed at Iranian nuclear program.

Non Military Domain

Georgia – 2008. Computer networks in Georgia were hacked by unknown hackers and annoying graffiti was posted on government web sites, coinciding with its standoff against Russia. Although no disruption of services took place, the incident put political pressure on the government. The attacks were coordinated with Russian military actions.

Dutch Certification Authority - September 2011. Unknown attackers hacked a Dutch certificate authority, allowing them to issue more than 500 fraudulent certificates for major companies and government agencies. The certificates were used to verify that a website is genuine. This was the second hack of a certificate authority in 2011.

INTERPLAY OF INFORMATION AND INTELLIGENCE WARS WITH IMPLICATIONS ON STATE SECURITY

Conceptual Frameworks - Information and Intelligence Wars

Concept of Information Warfare. Information warfare is defined as "*actions aimed at achieving information superiority by denying, exploiting, corrupting, or destroying the enemy's information and information functions, while protecting one's information and information functions against enemy attack*". Information warfare coupled with the invent of IT is becoming so sophisticated, that there is every possibility that in future it may be employed, as terrorist weapons in non-conventional sense by asymmetrical forces instead of regular armies.

Dimensions and Impacts of Information Warfare. Today, information warfare battle space is no longer confined to the military side but it now includes civil and public utilities. *Information warfare uses the information as primary weapon and attack at enemy recognition and information system*. Information warfare also controls the flow of information and intelligence and grasps the initiative in the battle field, in support of intelligence, psychological and electronic warfare. It also denies enemy the flow of information and creates false information to affect enemy perception of combat environment. Meanwhile, protecting own command and control system from enemy similar attacks.

Information-Intelligence Wars' Convergence into Fourth Generation Warfare with Implications on State Security

Conceptual Framework of 4th Generation Warfare. 4th Generation Warfare is defined as an "evolved form of insurgency that uses all available networks i.e. political, economic, social, and military to convince the enemy's decision makers that their strategic goals are either unachievable or too costly for the perceived benefit". 4th generation warfare is less about massing up force, to attack the enemy from outside and more focus is on under-winning the enemy from within. For this purpose, "state media, other sources of information and IT may come out to be the dominant operational and strategic weapon.

Manifestation of Fourth Generation Warfare. So far during 21st century, whatever is being witnessed in context of socio-political and economic disturbances is the manifestation of 4th generation warfare. Now *states are attacked by media, IT tools and employing of militants as a weapon of war and toppling of regimes*, while working behind the scenes. Currently, the wars being fought at militia levels in *Afghanistan, Yemen, Iraq, Mali and Syria* are the manifestation of 4th generation warfare.

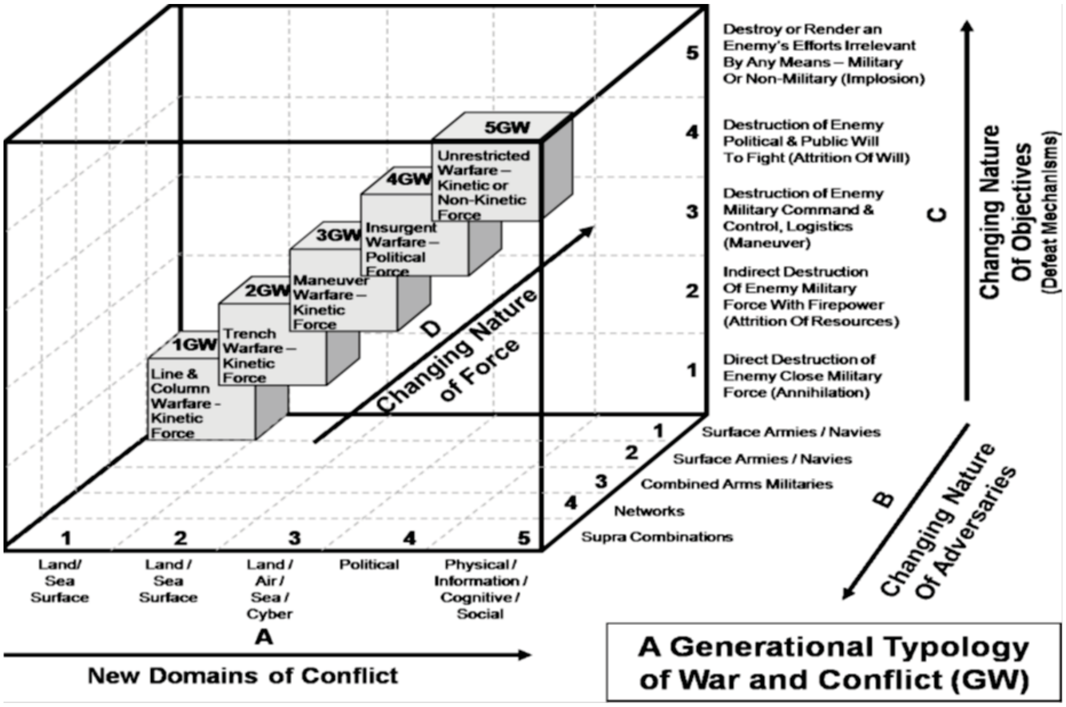
Application of Information and Intelligence Wars in Recent Times

Operation Iraqi Freedom. During Operation Iraqi Freedom, US forces augmented and sharpened their capabilities of technological networking in 2003. The rapid sharing of information at all levels of command was possible only because of the technologies US had in place thus, validated the concept of Net Centric Warfare.

Wiki Leaks Phenomenon. WikiLeaks, media organisation allegedly devoted to publish fact based materials, while keeping their sources anonymous. By the end of November 2010, WikiLeaks raised the stakes by starting to leak classified correspondence between US State Department and the US diplomatic missions. The documentation was leaked through five world class newspapers for a matter of credibility.

5th Generation Warfare. 5th generation warfare includes kinetic or non-kinetic attack on the political, social and military structures of the enemy in order to achieve strategic goals. More so, its *ultimate goal is same that of any war i.e. political defeat*. The figure - 2 below further elaborate the concept that first three generations of warfare (1GW, 2GW and 3GW) remained *kinetic in nature;* whereas, 4th generation warfare (4GW) showed major *tilt towards non-kinetic approach through insurgent warfare i.e. political domain* of warfare. On the contrary, 5th generation warfare (5GW) is considered *"Unrestricted Warfare" by employing combination of kinetic and non-kinetic forces* to destroy or render an enemy's efforts irrelevant by any mean i.e. military or non-military.

Figure 2: 5th Generation Warfare


1GW
Line & Column Warfare - Kinetic Force
2GW
Trench Warfare – Kinetic Force
3GW
Maneuver Warfare – Kinetic Force
4GW
Insurgent Warfare – Political Force
5GW
Unrestricted Warfare – Kinetic or Non-Kinetic Force
D
Changing Nature of Force
5
Destroy or Render an Enemy's Efforts Irrelevant By Any Means – Military Or Non-Military (Implosion)
4
Destruction of Enemy Political & Public Will To Fight (Attrition Of Will)
3
Destruction of Enemy Military Command & Control, Logistics (Maneuver)
2
Indirect Destruction Of Enemy Military Force With Firepower (Attrition Of Resources)
1
Direct Destruction of Enemy Close Military Force (Annihilation)
C
Changing Nature Of Objectives
(Defeat Mechanisms)
1
Surface Armies / Navies
2
Surface Armies / Navies
3
Combined Arms Militaries
4
Networks
5
Supra Combinations
B
Changing Nature Of Adversaries
1
Land/ Sea Surface
2
Land / Sea Surface
3
Land / Air / Sea / Cyber
4
Political
5
Physical / Information / Cognitive / Social
A
New Domains of Conflict
A Generational Typology of War and Conflict (GW)

MEDIA AS STAKEHOLDER IN STATE SECURITY SPECTRUM

Influence of Media on State Policies, Politics and Security

Changes in Policy Making Process. Information revolution has completely changed the policy making process, conduct of diplomacy and understanding of state security. Today, interstate opinions get influenced by the media; which subsequently influence the world leaders. Their pressure can even alter security strategies of countries and other interstate bodies. *Media warfare is pre-eminently a democratic instrument fashioned to dominate the mass minds, general will and sense of security of nation.*

Promotion and Projection of State Policies. Media is an important tool to promote and protect state policies. During post 9/11 period, US media has almost become a partner of the Pentagon in promoting and projecting the officially certified truth, even at the cost of its credibility and professional ethics. The newspapers which are reputed for their independence have been admitting in print that some of their reports were distorted even forged and based on factual inaccuracies.

Media and Information Warfare. Information warfare has become the catchphrase in the recent strategic thinking. It is now widely recognized that *information forms the 5th dimension of war*; along with land, space, sea and air. Though information is a valuable resource now, but its dissemination through the media has important bearing on state and inter-state security. Gulf Wars have proved how information could be used both as a military target and as a weapon.

Conflict Resolution. Media's role in interstate relations is vital, because it governs the ability of states to resolve disputes peacefully, which have direct bearing on country's security and prosperity. The mass media have the ability and capability to play effective role in altering interstate public opinions in making them better understood, in generating the will to solve them, and equipping people, if necessary, to put pressure on authorities to implement solutions.

Application of Media in Contemporary Era

Media-Military Relationship in Information Regulation. In contemporary era, military alone cannot achieve the political aim thus reliance on non-kinetic means especially media is essential to ensure success. Information operations are designed to manipulate the available information in a manner that regulation is ensured through media. Here, connivance of media is essential to ensure that only the intended information or dis-information is fed to the target audience.

Media in Non-kinetic Warfare. Advancement in technology has led to proliferation of information tools for exploitation by both parties to a conflict. State which previously felt dominant in any conflict is now being threatened by non-state actors. Information tools can be as profitably exploited by a non-state actor as a state would do therefore; monopolies previously experienced are no more valid now. Any side having dominance in media and information spheres is likely to have upper edge in prosecuting a successful non-kinetic campaign.

Role of Media in Perception Management. Abraham Lincoln said "Public opinion is everything. With it nothing can fail, without it nothing can succeed". *The power of media lies in its ability to transform perceptions into convictions*. Media creates attitudinal, emotional, physiological and behavioural effects.

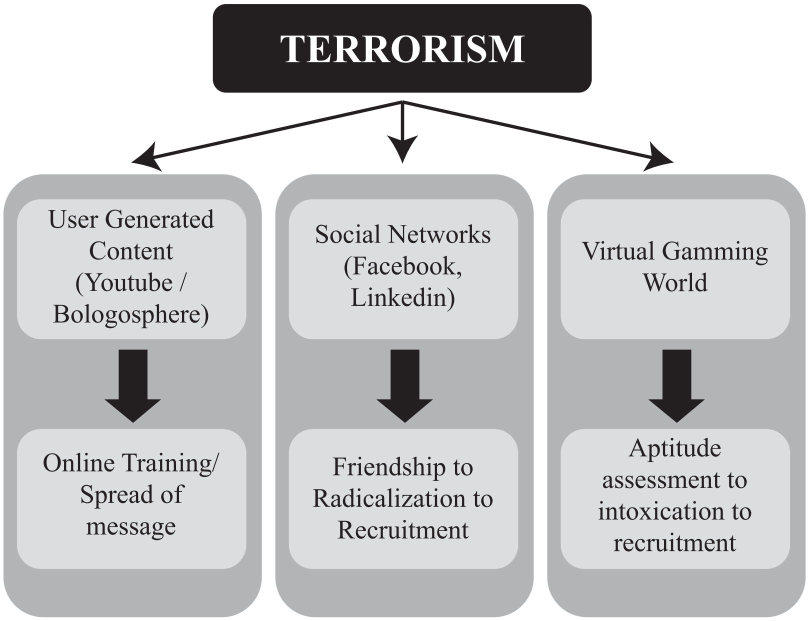
Social Media

Social Media. Social Media is an online environment established for mass collaboration. Social media is also a means of communication and marketing, made possible by the use of tools on the web etc.

Impact of Social Media on State Security

Communication Medium for Terrorist. Worldwide at large terrorist organisations are using social media to spread their ideology. They also communicate techniques of terrorist tactics, weaponry, improvised explosive devices and coded sharing of terror plans and activities. A virtual spread showing the use of social media by terrorist networks is illustrated below:

Figure 3: Social Media & Spread of Terrorism


TERRORISM
User Generated Content (Youtube / Bologosphere)
Online Training/ Spread of message
Social Networks (Facebook, Linkedin)
Friendship to Radicalization to Recruitment
Virtual Gamming World
Aptitude assessment to intoxication to recruitment

Discontentment cum Pollution of Minds. Social media contributes positively in creating awareness amongst masses of their rights however, it is also used negatively to spread discontentment. A lot is being done by states and non-state actors to further their objectives. China in recent years has been subjected to such efforts by various actors. Arab Spring can be quoted in the same context.

Operational Security. Widespread and easy access of the social media on mobile devices has made this media a threat to the operational security. Users (defence personal) may share some inadvertent information, which may jeopardize the whole operations.

Strategic Response Framework. A comprehensive strategic response should be all inclusive and based on four major strands:-

Preventive Strategy. Laws should be enacted to deal sternly with perpetrators of extreme ideologies, discontentment, maligning image of any religion, ethnic and sectarian trends. Search engines and social media administrators be engaged to ensure that country related portals remain sanitized according to the laws of the land.

Defensive Strategy. Integration of physical and virtual security means to enhance state security by employing physical security of the infrastructure along with enhanced redundancy of data bases through multiple backups. Also ensures high-technology access control system, advance security protocols apart isolation of vital databases and networks.

Offensive Strategy. Create cyber units not only to counter cyber offensive but also to exploit opportunities of affecting the hostile countries and non-state actors and neutralize their agendas. Enhanced footprint in social media through creating own social networks and blogs to protect minds of own youth and influence the mindset of the hostile actors.

RECOMMENDATIONS

Awareness of Information Revolution. Characteristics and impact of information revolution should be included in all high school curriculums. Moreover, it should also be made obligatory upon state media channels for awareness campaign.

Addressing the Vulnerabilities. A special project may be undertaken to assess the information and IT related vulnerabilities of the country. Accordingly, protection and remedial measures be launched under a comprehensive master plan to eradicate the gray areas and weak spots along with development of information warfare capability as part of future development strategy.

State Cyber Warfare Policy. State security is no longer restricted to mere defence of the borders, but is related to all elements of state power. Thus, cyber warfare has become closely related to state security. As a first step, there is a need to formulate a comprehensive "State Cyber Warfare Policy" by all countries to cater for transition into information age with emphasis on IT education.

National Information Security Policy. Each government around the globe needs to chalk out "National Information Security Policy". The government through policy implementation should ensure that all communication and computers setups must be shielded against enemies' cyber warfare system.

Cyber Discipline. Cyber discipline and technologies should be introduced in civil and armed forces institutions. This should be done with a view to broaden the base by developing the talent for subsequent employment of defensive and offensive cyber warfare capability.

Grand Strategy at Political and Military Levels. Political and military leadership must adopt a unified grand strategy, so that all components of government and military are aligned towards achieving the common goal of defeating a 4th generation warfare opponent.

Reduced Role of Non-state Actors. The emergence of multiple non-state actors has weakened the writ of the states throughout the world. The nations of the world through mutually agreed policy initiatives and measures should strengthen the state, which is considered more rational and responsible actor.

Media Strategy. There is a dire need for a comprehensive media strategy, which clearly defines the rules of the game and code of conduct/ethics. However it should not be seen as an attempt to impose censorship and curb freedom of media.

Force Multiplier in Non-Kinetic Domain. Government and armed forces need to work out how the media is to be exploited and harnessed to play its part in the exterior manoeuvres, and information warfare. The armed forces should be able to fully utilize the media as a force multiplier, in collaboration with all instruments of state power at the highest level based on a well thought out plan.

CONCLUSION

Information revolution is a paradigm change and has impacted state security. At the same time information age offers both opportunities and challenges. Weak state institutions are vulnerable to negatives of information revolution. However with enterprising population; one can accrue remarkable benefits from information revolution. Information assumes the place of an *element of state power*; which is critical to the present and future state security strategies. Information operations are more than technology; it is fundamentally a human-centric issue targeting the very security mechanism and structures of the state.

Cyber wars are real due to existing design of internet, flaws in software and hardware apart allowing critical machines to be controlled from cyber space. Moreover, cyber wars are fast thus, presenting a dilemma for decision makers; wherein the time between the launch of an attack and its effects is barely measurable. The world is slowly but surely graduating into the threshold of overt cyber attacks. Therefore, there is a need to have cyber arms control and informal rules of the “norms of acceptable behavior in cyberspace” by all nations. Militaries may not use cyber wars in isolation but as part of some larger military conflict as this alone cannot win a war. However, it is likely to cause major disruption in the functioning of critical infrastructures or system. Majority of government and armed forces of world have shown a cursory treatment to the threat spectrum of cyber security and yet to evolve a comprehensive strategy.

Information and intelligence have played crucial roles in winning past wars. All political and military strategists have emphasized the necessity of right kind of information and intelligence, about oneself and that of enemy, as decisive element in determining the fate of wars. The elements of information and intelligence has got great importance in modern conventional and insurgency related wars. During the first decade of 21st century, even the modern means of information and intelligence were challenged, as the insurgents, came out with much better experts in countering information and intelligence. Fourth generation warfare has come out to be a totally new phenomenon with very expanded and polarized dynamics in socio-political, economic and military perspectives, which can only be tackled, after dissecting the minuteness and delicacy of this war.

Wars are becoming increasingly asymmetrical and their results and time can no longer be predicted with any certainty. Introduction of non-state actors and more reliance on non-kinetic means has profound effects on the prosecution of war in contemporary era. From Gulf War-1 onwards, it is no longer possible to isolate the war zone from the media. This notion therefore, though workable in the past, is no longer an option. With increasing awareness and education, the nations are more likely to subject any war effort to a more critical analysis and base their support on that analysis, rather than blindly supporting the government and military. This highlights the importance of influencing public opinion positively through favourable media coverage. Individuals handling vital state secrets and operational security matters have direct access to social networking tools and are liable to inadvertent disclosure of the same on social media. This imperils the state security.

BIBLIOGRAPHY

Books and other Related Papers

1. A Detica White Paper, *An Operational Model for More Effective Cyber Security*. (UK: Detica Ltd, 2009). [Updated 15 November 2010; cited 26 January 2011].

2. Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Assistant Secretary of Defense (C3I/Command Control Research Program) Washington DC, 2000.

3. Aldrich, Richard W. *The International Legal Implications of Information Warfare*. No. INSS-OP-9. Air Force Academy Colorado Springs Co (1996).

4. Andy Jones et al., Global Information Warfare: How Business, Government, and Others Achieve Objectives and Attain Competitive Advantages (Florida, Auerbach Publications, 2000), p 55.

5. Andy Jones et al., Global Information Warfare: How Business, Government, and Others Achieve Objectives and Attain Competitive Advantages (Florida, Auerbach Publications, 2000), p 419.

6. Anthony H. Cordesman and Sam Khazai, *Iraq after US Withdrawal: US Policy and the Iraqi Search for Security and Stability.* Center for Strategic and International Studies (CSIS)

7. Byard Q. Clemmens, "Cyber warfare: Ways, Warriors and Weapons of Mass Destruction", Mil Review, September/October 1999, V.79, P.35.

8. Cited in Philiip M. Taylor, *Global Communications, International Affairs and the Media since 1945*, London, Routledge, 1997, p. 148

9. Col Thomas X. Hammes, *The Sling and the Stone* (St. Paul, MN: Zenith Press, 2004), p.2.

10. Commander Randall G. Bowdish, "*Information-Age Psychological Operations*", Mil Review, December 1998 - February 1999, p 32

11. Coskun Kurkcu. *U.S. Unmanned Aerial Vehicles (UAVs) and Network Centric Warfare (NCW): Impacts on Combat Aviation Tactics from Gulf War-I, Through 2007 Iraq*. Naval Postgraduate School Monterey,

12. Crawford, George A. *Information Warfare: New Roles for Information Sys in Mil Operations*. Department of the Air Force Washington DC, 1997.

13. David E. Johnson. *Preparing and Training for the Full Spectrum of Military Challenges*. (Santa Monica: RAND Corporation, 2009), p 198.

14. David S. Alberts and Daniel .S Papp: *The Information Age: An Anthology on its Impact and Consequences* (CCRP Publication Series, 1997)

15. Definition from "*Proceedings of Seminar on "A Maritime Strategy for India*" 1996. National Defence College, Tees January Marg, New Delhi, India.

16. E S Herman, "*The Media's Role in US Foreign Policy*", Journal of International Affairs (Summer 1993)

17. Emery, Edwin and Michael Emery. "*The Press and America",* Englewood Cliffs, N.J. Prentice-Hall, 1978, p 27

18. Falsehood in War Time*: Containing an Assortment of Lies Circulated Throughout the Nations During the Great War*, Kessinger Publishing, 2005.

19. Frank Webster's (1997: 27)

20. Information Operations: *The Fifth Dimension of Warfare*, Remarks as Delivered by Gen Ronald R. Fogleman, Air Force Chief of Staff, The Armed Forces Comms-Electronics Association.

21. James J.F Forest, *Influence Warfare: How Terrorists and Governments Fight to Shape Perceptions in a war of Ideas,* London: Pentagon Press, 2010, p 28-39.

22. John L. Petersen, *Information Warfare: The Future," in Cyberwar: Security, Strategy and Conflict in the Information Age*. Campen et al. (Fairfax, Virginia: AFCEA International Press, May 1996), p 221.

23. Juerg Studer. *Are There Five Rings or a Loop in Fourth Generation Warfare?* A Application of Warden's or Boyd's Theories in *Fourth Generation Warfare*. Air Command & Staff College Air University. Maxwell Air Force Base, Alabama April 2005.

24. Kenneth C Laudon and Jane P Laudon, *Management Information Systems*, (Prentice-Hall of India, New Delhi-110 001, 1998), P 7

25. Kuypers, Jim A. *Bush's War: Media Bias and Justifications for War in a Terrorist Age*. Rowman & Littlefield Publishers, Inc (2006).

26. Lord Jopling: Draft General Report on *Information and National Security*, NATO Parliamentary Assembly, October 2011.

27. Lt Col Lionel D. Alford," *Cyber Warfare: A New Doctrine and Taxonomy*". [Updated 18 December 2010; cited 26 January 2011]

28. M A Rice and A J Sammes, "*Communication and Information Systems for Battlefield Command and Control*", Brassy's (UK), 1989, P 4

29. Marina Caparini, *Media in Security and Governance: The Role of the News Media in Security Accountability and Oversight*, (Baden: Nomos, 2004), p 16.

30. Maud S. Beelman, *The Dangers of Disinformation in the War on Terrorism, Coverage of Terrorism Women and Journalism: International Perspectives*, from Nieman Reports Magazine, Winter 2001, Vol. 55, No.4, p.16. (from The Nieman Foundation for Journalism at Harvard University)

31. Max Boot, *War Made New: Weapons, Warriors and the Making of The Modern World*, (New York, Penguine Group (USA) Inc., 2007), p 469.

32. Michael Moore, *The Official Fahrenheit 9/11.* Reader, Simon and Schuster (2004)

33. Milan N. Vego. *Joint Operational Warfare Theory and Practice and V2, Historical Companion*. (Newport: United States War College, 2010), p 49- 53.

34. Myriam Dunn, "*A Comparative Analysis on Cyber Security Initiatives Worldwide*", WSIS (World Summit on Information Society) Thematic Meeting on Cyber Security, Centre for Security Studies, Zurich, 2005. [Updated 26 December 2010; cited 26 January 2011]

35. Myriam Dunn, "*A Comparative Analysis on Cyber Security Initiatives Worldwide*", WSIS (World Summit on Information Society) Thematic Meeting on Cyber Security, Centre for Security Studies, Zurich, 2005. [Updated 26 December 2010; cited 26 January 2011].

36. Rai Ajay K, *Conflict Situation and the Media, Strategic Analysis*, Vol XXIV, No 3, June 2000

37. RC Mishra, *Information Warfare and Cyber Security* (Delhi: Authors Press, 2003), p 122.

38. RC Mishra, *Information Warfare and Cyber Security,* Delhi: Authors Press 2003), p 125.

39. RC Mishra, *Information Warfare and Cyber Security,* Delhi: Authors Press, (2003), p 122

40. Richard A Clarke and Robert K Knake, *Cyber War*, (Harper Collins Publications, USA 2010), p 99.

41. Stephen E. Frantzich, *Citizen Democracy: Political Activists in a Cynical Age*, Rowman & Littlefield (2005)

42. The Implementation of Network-Centric Warfare. USA: United States. Dept of Defense (DoD). Office of Force Transformation 2010), p 29-30.

43. Vassiliki N. Koutrakou. *Contemporary Issues and Debates in EU Policy: The European Union and International Relations.* (New York: Manchester University Press, 2004), p 38.

44. Walter Laqueur. *A World of Secrets: The Uses and Limits of Intelligence*. (New York: Basic Books), p 8.

45. Webster, Frank. "*Information Warfare in an age of Globalization War and the Media: Reporting Conflict"* 24, no. 7 (2003): p 57-69.

46. Websites/Intrnet References/Documents

47. http://technologyploicy@csis.organisation. Accessed April 11, 2014.

48. http://blogs.Gartner.com/anthony_bradley/2011/03/08/defining-ocial-media-mass. Accessed May 20, 2014.

49. http://csis.organisation/files/publication/120702Iraq. Accessed on May 10, 2014.

50. http://en.Wikipedia.organisation/wiki. Accessed March 20, 2014.

Author

Brigadier Basit Raza is a Course Member of National Defence Course - 2014. He was commissioned in Pakistan Army in 1985 from Pakistan Military Academy. The officer is a graduate of Command and Staff College, Quetta, Pakistan and National Defence University, Islamabad, Pakistan. He has rich blend of Command, staff and instructional assignments. and has attended courses and senior officers training programmes at home and abroad. He served as Military Observer in UN Mission Sierra Leone. In pursuit of higher education the officer holds Masters degree in War Studies from National Defence University, Islamabad, Pakistan and also Masters degree in International Relations from Peshawar University, Pakistan. He is married and blessed by a daughter and a son. His hobbies include interior designing and reading.