Understanding information warfare and its relevance to Pakistan

Khurshid Khan *

Abstract

The use of Information and Communication Technologies (ICTs) in warfare scenarios has been central to the interest of governments, intelligence agencies, computer scientists and security experts for the past two decades. Information Warfare (IW) is the use of ICTs with either offensive or defensive purpose to immediately intrude, disrupt, or control the opponent's resources. While IW is as old as military history, the revolution in communication sciences has changed its nature. It has become a double edged sword equally important for the powerful states as well as technically poor states, non-state actors and individual expert in software. Some countries especially Russia and the US have taken a serious view of the IW technology and equated it with the threat of Weapons of Mass Destruction (WMD). In South Asian context, Pakistan is under direct threat of IW being applied by India in close cooperation with Israel. In addition, the Western media presents a very pessimistic view of Pakistan's economy, law and order and governance issues. Pakistan's armed forces and its intelligence agencies are the primary target of the propaganda warfare campaign launched by the national media duly sponsored by foreign actors. Nevertheless, IW has become a global threat thus, requiring a global remedy. At the national level, Pakistan will have to develop a proactive policy so that it can gear up to meet the crises which might emerge as a result of IW attack on its communication infrastructure specifically designed to keep its nuclear assets operational.

Introduction

The history of Information Warfare (IW) dates back to the history of mankind. Conflicts with more intensity are likely to continue unabated. Those who had swift access to the best information and were able to act timely were usually the victors in the battle.[1] Because of this reason, the proponents of IW often like to quote Sun Tzu's famous maxim, "Know the enemy and know yourself, then in a hundred battles you will never be in peril".[2]

* The writer is Director, Internal Studies, Research, & Publication, Institute of Strategic Studies and Research Analysis (ISSRA), National Defence University, Islamabad.

However, the 21st century has brought some exclusive dimensions to the art of warfare. The future wars between states and between states and non-state actors will be crucially dynamic in nature. The emerging patterns indicate that conventional war fighting capabilities might not prove very effective particularly in case of clashes between state and non-state actors or between two states where one is too weak. Therefore, in the age of IW, brains matter more than brawn. There is a perception that sub-state groups pose a particular problem as they may find it easier than states to exploit Information and Communication Technologies (ICTs) to leverage limited resources into disproportionate political, economic or military gains.[3]

In tomorrow's battlefield, be it military or civilian, information technology will act as a force multiplier. Traditional notions about the bases of superiority and power dynamics existing between attacker and the attacked may thus require redefinition.[4] While IW appears to be part of Fourth Generation Warfare (4GW), nonetheless; it is a powerful means that can also be applied single handedly to achieve the desired objectives of changing the mindset of the societies by impacting on their cultural, social and ideological values.

In the early 1990s, several people in the US Department of Defense (DoD) articulated a unique form of warfare termed as IW and a small cohort of defense scholars investigated the issue of cyber warfare. People's Liberation Army General Wang Pufeng wrote more than a decade ago, "In the near future, information warfare will control the form and future of war".[5]

One of the techniques used in IW is propaganda campaign which includes a planned dissemination of news, information, special arguments, and appeals designed to influence the beliefs, thoughts, and actions of a specific group. In the 1990s, the historian Oliver Thomson defined propaganda broadly to include both deliberate and unintentional means of behavior modification, describing it as "the use of communication skills of all kinds to achieve attitudinal or behavioral changes among one group by another".[6]

Though, there is no universally agreed definition of IW; Grumman has outlined a simple definition that says, "The ability to exploit, deceive, and disrupt adversary information systems while simultaneously protecting our own".[7] The general working definition of IW is, "IW is a coherent and synchronized blending of physical and virtual actions to have countries, organizations, and individuals perform, or not perform, actions so that your goals and objectives are attained and maintained, while simultaneously preventing competitors from doing the same to you".[8]

IW is a higher level, cerebral activity. The target can be a population, such as the national will or a specific political, religious, or ethnic group, a despot, a general, or anyone in an organization.[9] Simply put, IW implies a range of measures or "actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary".[10]

Currently, Pakistan has become a target of IW, deliberately used by the West in close collaboration with India and Israel. The targeted areas in Pakistan have a broad spectrum including its sovereignty, territorial integrity, cultural identity, ideological and ethnic cohesion and most importantly the economy. Additionally, Pakistan's nuclear program as well as the strategic assets and its armed forces including its intelligence agencies have been selected as special targets for engagement through IW.[11]

During 2008/2009, when operation 'Rah-e-Rast' was launched in Swat and Malakand regions, a perception was created by the disinformation cells of the US as well as other Western media that probably Islamabad was falling into the Taliban's lapse. During this campaign, Taliban's capabilities were exploded out of proportion.[12] There is a general feeling in Pakistan that after failing to achieve the desired objectives in Khyber Pakhtunkhwa (KPK), international media duly supported by 'insiders' has shifted its attention towards Balochistan province which has strategic significance and is considered a "Gateway to Central Asian Republics". The militants in Balochistan with the support of foreign actors both in terms of money and training, are actively involved in causing law and order situation providing sufficient ground for the international media to build a platform for an independent Balochistan that may suit the international stakeholders.

In this backdrop, this brief paper aims at addressing the following areas: one, understanding IW; two, relevance of IW to Pakistan; three, the proposed way forward and finally the conclusion. The opinion expressed in this paper is that of the author and does not necessarily reflect the institutional views or the government policies on the subject. The paper takes into account the political and security implications of IW leaving out technical aspects of the subject. Additionally, the use of IW in the domain of the business sector is beyond the scope of this paper.

Conceptual Framework of Information Warfare

The only difference between historical examples and the present ones is technological difference.

Information Warfare (IW) can be inferred in the writings of Sun Tzu. The ancient Greeks, Genghis Khan, the Medicis, Jomini, von Clausewitz, Mao Tse Tung, Ho Chi Minh, Che Guevera, Fidel Castro, and Slobodan Milosovic all practiced IW. The only difference between historical examples and the present ones is technological difference. Though, Information Technology (IT) is not a requirement for IW, but it allows for communications, computing, and decision making in seconds rather than months.[13]

IW is an umbrella concept embracing many disciplines. Some of the terms used for various practices in the information realm include; information systems security; information assurance; information superiority; information warfare; information operations; information dominance; critical infrastructure protection; operational security; communications security; and computer security etc.[14] However, with the development in IT sector, the IW has become more complicated and challenging. IW attacks can go unnoticed for months, and sometimes never detected. An information warrior can find a back door anywhere in the world because of the interconnectivity and interdependencies of many infrastructures.[15]

Many modern nation-states agree with the US military perspective that information operations (IO), span the spectrum of conflict, from peace through operations other than war to war and then back to operations other than war and peace. The US military believes that IW is reserved for conflict. According to E. Anders Eriksson, "IW is increasingly listed alongside nuclear, chemical, and biological weapons as a potential Weapon of Mass Destruction (WMD) or at least as a weapon of mass disruption". However, he puts his argument correct and says that cyber threat, being part of IW, does not fall in the category of weapons of mass disruption, but can be termed as weapon of 'precision disruption'.[16]

In order to understand IW, some selected definitions have been explained in the following paragraphs. Martin Libicki, in his essay "What is Information Warfare?" explained that "seven forms of IW vie for the position of central metaphor: command and-control warfare (C2W), intelligence-based warfare (IBW), electronic warfare (EW), psychological warfare (PSYW), hacker warfare, economic information warfare (EIW), and cyber warfare."[17]

According to Winn Schwartau, "Information warfare is the use of information and information systems as both offensive and defensive tools (weapons) against adversaries." He breaks IW down into three classes. Class one is personal or, as he currently prefers, privacy. Class two is corporate or, again his current preference, espionage. Class three, from his earlier writings, is global. Today, he calls it terrorism. He further referred to another definition issued by the Secretary of Defense; IW is "… actions taken to preserve the integrity of one's own information systems from exploitation, corruption or destruction, while at the same time exploiting, corrupting, or destroying an adversary's information systems and in the process achieving an information advantage in the application of force."[18]

According to Lt. Col. Gregory Rattray, Commander of the US Air Force's 23rd Information Operations Squadron, strategic operations in cyberspace will be a major part of twenty-first-century warfare. Warfare in cyberspace should not focus, Rattray suggests, on the use of "information in warfare", but rather on "information warfare as a means for state and non-state actors to achieve objectives through digital attacks on an adversary's centers of gravity".[19] In that context, he focuses on the organizational structures and means necessary for computer attacks that can disrupt and destroy information infrastructures. In this context, he makes a compelling argument that IW at the strategic level offers both an opportunity and a threat.[20]

According to the definition given by a Pakistani scholar, IW is a type of Electronic Warfare which aims at neutralizing and obtaining information from, or monitoring enemy computer information systems and networks. Additionally, IW capability, in a defensive role, must provide adequate protection to 'own' systems and networks.[21] The Dictionary of Military and Associated Terms defines IW as, "Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries". IW is more than computer network attack and defense,[22] most effective when performed in a synchronized and coherent fashion that is why knowledge management complements it so well. All components of an organization, as well as across the enterprise, need to be included in an IW action plan. The purpose of IW is to control or influence the decision maker's actions. An area of control can be directly manipulated, whereas an area of influence can only be indirectly manipulated. Control and influence are the essence of power.[23]

Robert Ayers draws a comparison between IW and conventional war. He said that they are very different things - with different connotations and different

problems. In conventional war, we have visible battle space and we organize our military forces around this geography. IW, on the other hand, doesn't occupy a physical battle space; it's a logical battle space. When we fight conventional wars, we have identified adversaries but in IW, your enemy doesn't wear a uniform. In conventional war, you have time to mobilize but with cyber war which is the latest form of the IW, no mobilization is required. No deployment is required. It simply happens at the press of a button. [24]

He goes on to say, "In IW …we don't know how to play simply because when we're engaged in a war against the adversary that may not be a nation state".[25] Similarly, while we can distinguish between conventional and nuclear attacks, IW may turn out to be a seamless process that begins as one small-scale episode and steadily escalates all the way to large-scale attacks with effects comparable even to nuclear attacks as explained by Blank in one of his articles.[26] A typical goal of conventional warfare is to destroy or degrade the enemy's physical resources, whereas the aim of IW is to target information assets and infrastructure. In the information age, the silent enemy can easily acquire a voice and quickly amplify its dissident message.[27]

John Arquila and David Ronfeldt come up with another definition of the IW which says, "The information revolution will cause shifts both in how societies may come into conflict, and how their armed forces may wage war. We offer a distinction between what we call 'netwar'– societal-level ideational conflicts waged in part through inter-netted modes of communication and 'cyberwar' at the military level".[28]

While there are other analysts and scholars in China working on IW, Dr Shen Weiguang, is considered the father of Chinese IW. These analysts provide definitions and insight into IW with a distinctly 'Chinese' flavor slightly different from the US thinking. To the Chinese experts, IW means 'Information War' rather than 'Information Warfare' as viewed by the US thinkers. Most American military experts consider IW as a way of fighting; hence the term warfare is used, where as Chinese experts look at IW as the fight itself. Chinese IW specialist General Wang Pufeng summed it up and stated that 'Information War refers' to a kind of war and a kind of war pattern, while Information Warfare' refers to a kind of operation and operational pattern.[29]

Dr Shen also provided a broad definition of IW as a war in which opposing groups vie for information space and compete for information resources. He believes that the essence of IW is to force your enemy to surrender without having to fight by using information superiority.[30] To the Chinese expert, IW is not limited to times of conflict or crisis, but is ongoing. Dr Shen defines two

types of war: the violent kind that occurs on the battlefield, and its non-violent opposite, which he defines as ‘‘deterrent war.’’ The violent type is temporary in duration and usually limited in scale. But deterrent war occurs off the battlefield, and takes up all the ‘‘space and time’’ not covered by violent war. He postulates that, in deterrent war, opposing forces convert their power into information and deterrence. This conversion of power invariably leads to IW in a number of areas as efforts focus on stopping or altering an opponent’s ‘‘belligerent behavior.’’ Thus, IW is an ongoing battle fought on several planes to various degrees.[31]

Colonel Wang Baocun expanded on the idea of IW being an ongoing operation. He described the ‘‘Forms of IW,’’ as peacetime, crisis, and wartime. Author Liang Zhenxing stated that IW included all types of war fighting activities that involve the exploitation, alteration, and paralysis of an enemy’s information and information systems, while protecting one’s own similar systems. He believes that the essence of IW is to render the operational space unclear or indistinct to enemy forces and transparent to one’s own forces. This was one of the first Chinese definitions to highlight the defensive, as well as the offensive, nature of IW.[32]

In theory, a small team of hackers (even a lone operator) can wreak havoc, whether the target is military or civilian. It is because of this reason that the US was compelled to establish the Commission on Critical Infrastructure Protection.[33] Therefore, it is not only the West which can wage information campaigns; rather it is not at all certain that the West is actually expert in this aspect of warfare in the strategic arena that really counts.[34]

IW constitutes a double-edged sword for information-intensive nations like the US. The greater the military’s reliance on complex networks and smart weaponry, the greater is its potential vulnerability to stealth attack by materially much weaker enemies blessed with networking savvy. Moreover, ‘information’ is also a double-edged weapon because it benefits, strengthens, and enhances the operational effectiveness of non-conventional forces as much as or more than it does so for conventional forces. This is a sword that cuts both ways. In addition, there is the absence of early warning and the difficulty of knowing whether, or to what extent, one’s systems have been penetrated and compromised.[35]

For a brief period during the 1940s and early 1950s, the terms “psychological warfare” and “political warfare” were openly adopted by propaganda specialists and politicians alike. Increasingly, they turned to euphemisms like “international communication” and “public communication” to

make the idea of propaganda more palatable to domestic audiences. During the Cold War, common phrases also included "the war of ideas", "battle for hearts and minds", "struggle for the minds and wills of men", "thought war", "ideological warfare", "nerve warfare", "campaign of truth", "war of words", and others. Later on, the terms "communication", "public diplomacy", "psychological operations", "special operations", and "information warfare" became fashionable. Political propaganda and measures to influence media coverage were likewise labeled "spin", and political propagandists were "spin doctors" or, more imaginatively, "media consultants" and "image advisers".[36]

IW is not about a one-time silver bullet for a quick fix, neither is it restricted to using computers to attack other computers nor confined to the cyber-realm. When properly employed, IW is an agile capability that can be tailored to any situation. It can bring a multitude of functions to bear. IW can be implemented in the physical and virtual worlds. Central to IW is how it is used to influence decision makers. Magazines, radio, television, newspapers, leaflets, e-mail, Web pages, and other forms of media can all be used as a vehicle to deliver IW.[37]

IW cuts across national borders, educational backgrounds, and cultural views. It enables direct and indirect attacks from anywhere around the world in a matter of seconds. Physical proximity to the target is not necessary. This has become possible because we have made conscious and unconscious decisions to have speed and connectivity without complementary security. In Sun Tzu's and Genghis Khan's eras, physical, personnel, and operational security were all that was needed for protection. Today, we have fiber optics, satellites, personal digital assistants, infrared and laser communications, interactive cable television, mobile phones, and a host of other technological marvels that allow us to reach anywhere in a few seconds.[38]

From the author's perspective, no simple sentence or paragraph can effectively describe IW which is a very complex concept. IW being an umbrella term plays a decisive role at two levels. At operational level, with the help of computers, software, and the Internet (and intranets), one side might paralyze the communication, command and control infrastructure of its adversary through enhanced efficiency, speed, and coverage. This might be done for a limited duration. At the strategic level, IW has a greater role in achieving the grand objectives. It is applied across the target state for a longer duration making possible the use of all available tools including propaganda and psychological operations inside the country and across the globe through diplomatic circles. Print and electronic media has become one of the best means to promote the selected narratives/themes against the target country through perception making. In the author's candid view, since the last many years,

Pakistan remains central to the IW campaign being launched by insiders and outsiders to weaken it, both economically and militarily.

The leading belligerents powers of World War I were engaged in IW throughout the war at a scale never imagined earlier.

The leading belligerents powers of World War I were engaged in IW throughout the war at a scale never imagined earlier. Both sides (UK and Germany) understood the importance of information control to warfare as a force multiplier. Moreover, they did not limit their focus to the military applications of information to battle, but expanded it to the wider role of information as a commercial, financial, or diplomatic tool in the larger geostrategic environment. During the war, UK had suppressed Germany's worldwide cable and radio network and imposed an information blockade on it by developing signals intelligence processing capability. However, despite technical limitations as compared to UK, German's also launched attacks against the communication network of its enemies including the US.[39]

As highlighted earlier on, IW in the electrical age is not a new phenomenon but dates back to the late nineteenth century. There are several instances in this period where belligerent powers deliberately targeted submarine telegraph cable systems for attack or signals interception through censorship.[40] It is now believed that IW is vital to current military operations and that such attacks may represent a potential strategic vulnerability to a nation's critical infrastructure.[41] The nature of the projected IW threat seems very serious. Timothy Thomas, a US official quotes Russian sources who view that IW as a strategic threat is comparable to nuclear weapons in their functional outcome.[42] A Russian study of soldiers of the future concluded:

> Ideologically these developments are based on the concept of an "information war", created on the basis of the latest achievements of scientific and technical progress and with an associated revolution in military science at the turn of the XXI century. By its consequences, it is possible to compare it only with the creation of nuclear weapons in the middle 1940s. The introduction of information- space technology at all levels of control and troop applications actually make it possible to seriously speak about the possibility of "combat operations in digital form.[43]

Russians have taken this threat so seriously that they have suggested to the United Nations to launch a process by which it could devise an international agreement to ban IW. Ivanov argued that IW's destructive potential was

tantamount to that of strategic nuclear weapons and therefore, it should be banned. Most Russian's writing on the subject points to the conclusion that Moscow would respond to an IW attack much as it would to a nuclear attack, i.e. by a nuclear counter-attack.[44] As the Russians argue, a successful attack on an information network could inhibit the launching of a nuclear response or an equally destructive IW equivalent of the second strike, or it could so disrupt the governance of a state as to render it ungovernable.[45]

As a result of the detailed study conducted by Peter Stephenson, he concludes that beyond all the hype of IW, it held one significant hope: it might raise awareness of real threats against information assets to a point where organizations actually started spending money to protect their most important asset, "the information".[46] One thing is certain that threats are real and accordingly, the advanced countries in particular and the developing countries especially with nuclear weapon technology in general have started investing huge money to protect sensitive information.

Relevance of the Information Warfare to Pakistan

As stated earlier, Cyber warfare is the latest form of IW. IT dependence in the US is evolving into a strategic center of gravity. This represents an inviting target to a potential adversary. Cyber threat has become a global phenomenon where the US and China seems engaged in this war and continue to spend millions of dollars. Similarly, the US and Israel are also found intruding into Iran's nuclear program. There is a serious tension between China and India too. The Internet security company McAfee stated in their 2007 annual report that approximately 120 countries have been developing ways to use the Internet as a weapon.[47]

In South Asian context, Pakistan being a developing country lacks requisite technological expertise in the field of IW and presents itself as a most attractive target to its adversaries. It is not prepared to respond to this latest threat likely to be launched by its adversaries. As pointed out by Charles Billo and Welton Chang:[48]

> The Indian authorities announced a shift in military doctrine in 1998 to embrace electronic warfare and information operations. An IT roadmap, enumerating a comprehensive ten year plan, was published. In the framework of the roadmap, the government has granted permission for closer government/industry cooperation to leverage the output of India's world-class IT software industry. In addition, a new National Defense University and Defense Intelligence Agency (DIA) have been established. According to

> journalistic accounts, the armed forces plan to establish an information warfare agency within the DIA with responsibility for cyber war, psychological operations, and electromagnetic and sound wave technologies.

India has all the capabilities/resources to launch Cyber attack against Pakistan's sensitive targets. As Israel has already joined hands with India, the threat level has gone further up.[49] Cyber warfare is fought on the cyberspace using weapons like cyber espionage, web vandalism, gathering data, distributed denial-of-service attacks (DDOS), equipment disruption, attacking critical infrastructure, compromised counterfeit hardware, and virus and worm release. The potential targets of this war are numerous including the military dimension.[50]

How eagerly the Indians want to gain an edge in cyber warfare technology is evident from what the Indian Naval Chief Admiral Sureesh Mehta told to *Start Post*;

> The Indian armed forces are increasingly investing in networked operations, both singly and in a joint fashion. We can't afford to be vulnerable to cyber-attacks. Information technology is our country's known strength and it would be in our interest to leverage this strength in developing a formidable 'offensive' and 'defensive' cyber warfare capability. Harnessing the gene pool available in academia, private industry and the younger generation of talented individuals is imperative.[51]

Though, no large scale cyber-attack has been reported in Pakistan, yet a number of limited cyber skirmishes have already taken place between the Indian and Pakistani hackers in the recent years as also between Palestinians and Israelis.[52] These minor skirmishes could become a potent threat if appropriate counter measures were not taken by Pakistan especially when Israel is also fully involved. However, the discouraging news is that currently, there is no mechanism available to deter IW attack. Even the US and the other potential future adversaries are also searching for an answer to this threat.[53]

India is keeping all its options open. It is also involved in destroying Pakistani culture and society as a whole through other means including its print and electronic media. The narratives have also been given to film media which is refueling the enmity for Pakistan. Historically, Indian film media has been involved in perception making that the creation of Pakistan which is based on 'Two-Nation theory' was an abortive idea. In addition to this, Muslims are being portrayed as terrorists and smugglers.[54] Moreover, India's film/TV media is fully involved in perception making in Afghanistan against Pakistan and they

have succeeded to a great extent in creating hatred against Pakistan despite colossal sacrifices made by Pakistan for the people of Afghanistan for over three decades. Today, Afghan people are seen siding with India against Pakistan.

Since the last few years, it has been observed that the websites of international newspapers, blogs and social networking sites such as facebook and youtube continue to project Pakistan negatively and deliberately discredited at international forums on one or the other plea. Consequently, a perception is being built that Pakistan is a failed state and a breeding ground for terrorist activities. Such propaganda campaign on multiple channels not only damages the image of the country but also de-motivate those analysts who intend to project Pakistan's soft image.

There is another area of serious concern related to the safety and security of Pakistan's nuclear program. The real concerns might emerge if the propaganda campaign launched against Pakistan's nukes proves true where it says that Pakistan's nukes could be made nonoperational as some of the American technicians have had direct access to the nuclear weapons.[55] Sale claims that one former senior US intelligence source shared the information with him and said, "In the course of such work, America gained "a pretty full knowledge" of Pakistan's command and control system".[56] It is not the US that seems worried about the insecurities of Pakistani nukes; Israel is also playing an instrumental role in propaganda campaign against its nuclear program. She has also setup a huge workforce of writers on the internet and is still increasing its strength. Primary task of this force would be to wage propaganda war against Pakistan and its nuclear weapons and armed forces. Hebrew websites and magazines have been targeting Pakistan by orchestrating near to impossible scenarios about the vulnerability of Pakistani nukes and the "possibility" of their falling into al-Qaeda hands. Israeli lobbies have been heavily exploiting their clout in US and UK to wage a propaganda war against Pakistan's nuclear program through satellite news channels. India also remained active and its political leadership took this disinformation war to new heights by saying that, "some of the Pakistani nuclear installations were already under Taliban control".[57]

The most effective and lethal weapon for precise and operative IW is local media and this includes paper, electronic and cyber. While cyber create impacts in a different perspective, media plays a decisive role in "perception management". Since the beginning of this century, the initiative was taken by General Musharaf to bring in private media for perception management inside Pakistan and around the world. But, no serious work was done to formalize the plan to set and enforce the rules of the game and code of conduct for regulation

before issuing license to the private media companies. There is no formal training institution for media personnel. A modest effort has been launched at the National Defence University, Islamabad which organizes 'National Media Workshop' once or twice a year. Thus, in the absence of guidance and a clear roadmap, it encouraged ingress of foreign elements in the ranks of media. Issuance of hundreds of media licenses without any check and balance has drowned us in deep waters. Modern journalists rightly claim, "Hundred guns silence a single camera but one camera can silence hundred guns".[58]

US has grand designs to weaken Pakistan to an extent that it willingly comes forward to extend its full cooperating with the US on all matters.

In the author's views, the perception of media in Pakistan as a state pillar is incorrect. It may have acted as a bulwark against wrong practices of the current regime but it has caused serious damage to Pakistan's image across the globe. In this context, Jawad Raza Khan raised an important question, "Can we develop the concept of private government machinery, can we think of having private judiciary working in courts and can our slightest imagination take us to a private Army fighting for the country…. it indeed sounds absurd".[59] Nevertheless, we should not be seriously worried because except for a small segment of literate conspirators, the entire Pakistani media works in harmony to ensure unity of the masses on all important security related issues including its support for the armed forces which was crucial in tackling the militants' in Malakand, Bajaur, Swat and Dir.

The author sincerely believes that the US has grand designs to weaken Pakistan to an extent that it willingly comes forward to extend its full cooperating with the US on all matters. Accordingly, it is involved in unfolding the strategy step by step targeting all sectors in collaboration with India and Israel. Pakistan's armed forces remained the strongest hurdle in its way to achieve its objectives, unless they are weakened, the US dream of unarming Pakistan can't materialize. Therefore, Pakistan armed forces continue to be targeted from multiple angles. They are involved in low intensity war in KPK and being dragged in Balochistan unrest as well. Additionally, they are also being targeted from few political circles.

The foreign media is prejudiced to Pakistan; it has never mentioned that Pakistan has sacrificed thousands of its citizens as well as security personnel in the war against terrorism. Nor has it revealed that Pakistan has handed over

several hundred al-Qaeda terrorists to the US. The media campaign is in full swing against the armed forces including their intelligence agencies which are expected to be the eyes and ears of a country. There is a deliberate effort to create dent between the political and military hierarchy. The reports in the UK media that General Kayani had secret meetings with Indian leadership on Kashmir issue are part of such conspiracies. BBC, CNN, Fox News are the biggest propaganda machines which brainwash the public to carry on their own agendas.[60]

In the author's opinion, while such an assault on Pakistan's prestigious institutions has become a common practice, indifferent analysis and negative commentaries through print and electronic media is over blowing such information which is creating misperceptions about its armed forces and intelligentsia. By weakening Pakistan's intelligence setup, international intelligence mafia including CIA, RAW, MI-6 and Mossad, is likely to have more ingress in the internal affairs of Pakistan.

Just a few months back, there was a deliberate IW attack which created a hype to give an impression that probably, Balochistan was breaking away from Pakistan. In reality, there are just few thousands misguided men from only 5 districts out of 30, duly sponsored by foreign hands.[61] But unfortunately, people have heard the interviews of Brahmadagh in media but would hardly hear the voice of Mir Ahmadan Bugti, a die hard Pakistani. The Balochistan problem has not been put in true perspective. The issue of missing personnel has also been mishandled. There is a massive infighting between the Balochistan Republican Army (BRA) and BLA where both groups are killing each other for weapons, money and turf and then blame the army for the murders. Additionally, many have gone to Afghanistan for training and their families register them as missing persons. This is all part of the propaganda campaign against Pakistan army and its intelligence agencies and regrettably, the media is fuelling it.[62]

The militants who are involved in cold blooded murder of the uniform personnel including Frontier Corps and Police are being encouraged. None of the international media has ever condemned their killing of uniform personnel as well as killing of over 1500 innocent non-Baloch residents over a period of last three years. But if the law breakers are killed in encounters with the law enforcing agencies, their death is considered as human right violation. International media is thus, involved in poisoning the Balochistan society, which has a long lasting negative impact.

Suggested Way Forward

There is no quick solution to the current and the emerging threats of IW. The threat is real but the remedy is doubtful and even the most advanced states including the US seem unprepared to respond to the IW attacks in an assured manner. IW is a global threat and it needs a global response. Thus, greater cooperation by all states especially those having state of the art technology need to extend full cooperation to less developed states. Collective efforts must be directed against non state actors and individuals with a view to discourage them from undertaking adventurous activities which have a devastating impact not only on the economic sectors but also on the nuclear field.

Defensive IW strategies are an effort to protect the system against theft, disruption, distortion, denial of service, or destruction of sensitive information assets. While pure defensive measures are important however, for a better response, resources must be invested in creating more effective intelligence and counterintelligence capability in an effort to anticipate likely attacks and their sources. In an age of economic and corporate IW, proactive intelligence management systems become essential requirement.[63]

We must understand that technology is developing rapidly. Even technically advanced countries including the US and UK seem ill prepared to catch up with the upcoming technology to defend their respective national infrastructure. Therefore, this being the most sensitive national security issue must be taken seriously. The nation states must be aware of the importance of being able to respond to an attack, be prepared for reconstitution, and know in advance how you are going to prioritize resources to get the national infrastructure back in service.

As highlighted earlier, the information revolution has fostered the rise of new ways of waging war which are primarily disruptive, rather than destructive; and its low "barriers to entry" make it possible for individuals and groups (not just nation-states) to easily acquire very serious war-making capabilities. Therefore, the nations and societies leading the information revolution have a primary ethical obligation to constrain the circumstances under which IW may be used – principally by means of a pledge of "no first use" of such means against non-combatants.[64]

Foreign policy based on cooperative security, increased mutual trust and agreement for 'non-use' of IW both at the global and regional levels especially between the rival states in possession of nuclear weapons is essential.

Domestically, legislation is important to evolve comprehensive policy to deal with non-state actors as well as other law breakers. All states and NGOs that have legitimate interests in coping with these threats should be taken on board.

Public policy has a proactive side, building infrastructure in the broadest sense of the word, is its reactive side. In the present context, infrastructure could include such items as standardization, legislation, international regimes, regulatory agencies, and structures for warning, alerting, and crisis response. The infrastructures should be built to manage a broad variety of potential future developments, the vast majority of which will never materialize. To do this will require extensive use of scenarios and other qualitative foresight methodologies. Furthermore, purposeful crisis response against an innovative adversary requires that the knowledge created in scenario exercises and forecasts on possible attack concepts be retrievable and useful to analysts.[65]

With regards to Pakistan, it can't afford any complacency. Therefore, all possible steps required to protect its conventional as well as nuclear assets should be taken immediately to respond to this lurking threat. It should be clearly understood that in the modern world, only those nations would have the advantage on the battle field, in both conventional and unconventional wars, which have fought and won the war in the cyber world first.

Weapons like E-bombs have already emerged as a new threat to cripple the military communication infrastructure by producing massive electromagnetic pulse. Pakistan must start working on Transient Electro Magnetic Pulse Emanations Standards, known as TEMPEST in military parlance to counter electromagnetic-pulse bombs that can interrupt wireless signals. Pakistan needs urgently to create a centralized, aggressive and pro-active command for cyber and IW under the Joint Command. It is very important that the unguarded flank of Pakistan's defence must be secured at the earliest.

The perception management platform needs to be thoroughly scrutinized as a priority, as anything short of that will minimize any good done in the right direction. The black sheep's are required to be handled with concrete parliamentary steps supported by the executives to ensure damage control. There is a dire need for some centralized means to train our media men through government institutions, where the thumb rule should be centralized planning to deal with information war crisis with de- centralized execution with precision and lethality.

With regards to Pakistan army, the ISPR needs to be proactive and must generate number of themes/ narratives to promote and protect its army as one of the most important pillar of the national security through print and media. It can't take a back seat. Reactive strategy would produce no result. In this day and age, it is difficult to suppress information; instead of hiding, efforts should be made to minimize the damage.

At the highest level, there is a need to develop an understanding that our country is confronted with numerous extraordinary challenges. It is very important to comprehend these issues in their true perspective rather than toeing the line of propagandists. While awareness is positive, the conspiracy theories weaken our convictions by spreading divisive themes and elusive schemes. The nation must maintain cohesive posture in the face of hostile propaganda. Domestic media has an important role in this context. It must be taken on board by confiding into its responsible managers so that it plays its role to dispel the present state of despondency, conspiracy theories and misperceptions. Pakistan's armed forces, one of the important pillars that protect national security should not be degraded. Therefore, national media must realize its significance and play a positive role in correcting perceptions and strengthening people's faith in the professional competence of Pakistan's armed forces.[66]

In order to counter India's propaganda campaign led by its film media, an effective policy needs to be created. In addition to the making of films about Kashmir and Pak-India relations, Pakistan must boycott all those Indian films, which are based on enmity for Pakistan. The efforts must ensure that the boycott is effective and in no way, the Indian films containing such propaganda enter into Pakistan via any media. An awareness program through Pakistani media is also important to make the general public understand India's motives behind such movies. Similarly, Pakistan should also launch an effective counter offensive in Afghanistan through its own media including movies/dramas so as to minimize the impact of Indian movies and other programs which are aimed at damaging Pakistan's image in Afghanistan.

Conclusion

IW is an all-embracing concept that requires managing all the resources of a nation–state or business organization in a coherent and synchronized manner to control the information environment, to attain and maintain a competitive advantage, and gain power and influence. Governments and the Corporate Sector can use IW offensively and defensively in the physical and virtual domains. Counters to IW do not have to be in-kind; they can be no, low, or high technology and they can be asymmetric. Although the name may change over

the years, but IW will evolve from its nascent stage and will become main stream in the coming two decades. IW is about synchronized coherent relationships and capabilities. The resources of its enterprise are brought to bear to use all its capabilities in a coherent and synchronized manner to seize as great a competitive advantage as possible. In this fashion, a country can call upon its allies and coalition partners, and a business can call upon its suppliers and business partners so that as much knowledge and as many capabilities as possible can be brought to bear.

Currently, Pakistan is passing through a critical phase as the nation is confronted with extraordinary challenges at internal and external levels. Defeatism and getting paralyzed is no option. Pakistan will have to defeat all kinds of IW campaigns launched by the 'outsiders' and 'insiders' by evolving a comprehensive 'Counter IW Strategy'. However, even a comprehensive plan may also fail if civil society including intellectuals and media does not put up a collective front to internal and external threats. Finally, being a nuclear weapon state, Pakistan can't afford to lower its guards with regards to Cyber threat to its nuclear assets. Thus, it is extremely important that Pakistan takes all necessary safeguards to ensure that its nuclear assets remain operational when required.

Notes & References

1 Andy Jones, Gerald L. Kovacich & Perry G. Luzwick, "Everything You Wanted to Know about Information Warfare but Were Afraid to Ask, Part 1", *Information Systems Security* 11, no. 4 (2002): 9-20, http://dx.doi.org/10.1201/1086/43322.11.4.20020901/38841.3, (accessed February 18, 2012).

2 Sun Tzu, *Art of War*, trans. S.B. Griffith (London: Oxford University Press), (1971), 84.

3 Andrew Rathmell, "Information Warfare and Sub-State Actors: An Organizational Approach", *Information, Communication & Society* 1, no. 4 (1998): 488, http://dx.doi.org/10.1080/13691189809358984, (accessed March 13, 2012).

4 Blaise Cronin, Holly Crawford, "Information Warfare: Its Application in Military and Civilian Contexts", *The Information Society: An International Journal* 15, no. 4 (1999): 257-263, http://dx.doi.org/10.1080/019722499128420, (accessed March 15, 2012).

5 Jones, Kovacich and Luzwick, "Everything You Wanted to Know about Information Warfare but Were Afraid to Ask, Part 1", 9 -20; Robert Ayers, "The New Threat: Information Warfare", *The RUSI Journal* 144, no. 5 (1999): 23-27, http://dx.doi.org/10.1080/03071849908446441, (accessed March 4, 2012); and Chris Bronk, review of the "Conquest in Cyberspace: National Security and Information Warfare", by Martin C. Libicki, *Journal of Information Technology & Politics* 4, no. 4 (2008): 89, http://dx.doi.org/10.1080/19331680801979054 (accessed March 23, 2012).

[6] Kenneth A. Osgood, *Encyclopedia of American Foreign Policy*, s.v. "Propaganda" (2002), www.encyclopedia.com/topic/propaganda.aspx (accessed March 17, 2012).

[7] Peter Stephenson, "Information Warfare, or, Help! The Sky Is Falling!", *Information Systems Security* 8, no.1 (1999): 6-10, http://dx.doi.org/10.1201/1086/43304.8.1.19990301/31046.2 (accessed February 19, 2012).

[8] Jones, Kovacich and Luzwick, "Everything You Wanted to Know about Information Warfare but Were Afraid to Ask, Part 1", 9 -20.

[9] Gerald L. Kovacich, Andy Jones & Perry G. Luzwick, "Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages, Chapter 1, Part 2", *Information Systems Security* 11, no. 5 (2002): 15-23, http://dx.doi.org/10.1201/1086/43323.11.5.20021101/39848.4, (accessed March 27, 2012); and Farzana Shah, " Propaganda & Warfare in Cyber World", *Pakistan Tribune*, August 2, 2011, http://paktribune.com/news/index.shtml?242277 (accessed February 11, 2013).

[10] Cronin and Crawford, "Information Warfare: Its Application in Military and Civilian Contexts", 257-263.

[11] Aashique Chaudhary, "Bollywood in Propaganda War against Pakistan", translation of an article from *Jang* (Rawalpindi), February 20, 2002, szh.20m.com/issues/bollywood.html (accessed March 17, 2012); and Shah, "Propaganda & Warfare in Cyber World".

[12] Shah, "Propaganda & Warfare in Cyber World".

[13] Jones, Kovacich and Luzwick, "Everything You Wanted to Know about Information Warfare but Were Afraid to Ask, Part 1", 9 -20.

[14] Ibid.

[15] Ibid.

[16] E. Anders Eriksson, "Viewpoint: Information Warfare: Hype or reality?", *The Nonproliferation Review* 6, no. 3 (1999): 57, http://dx.doi.org/10.1080/10736709908436765 (accessed March 14, 2012).

[17] Ibid.

[18] Ibid.

[19] Blaise Cronin, review of the "Strategic Warfare in Cyberspace", by Gregory J. Rattray, *The Information Society: An International Journal* 19, no 4 (2003): 14; Grenier John, review of "Strategic Warfare in Cyberspace", *Technology and Culture* 44, no. 1 (January 2003): 190-191 (Review), DOI: 10.1353/tech.2003.0015, (accessed April 12, 2012).

[20] Grenier John, "Strategic Warfare in Cyberspace", 190-191.

[21] Syed M. Amir Husain, "Pakistan Needs an Information Warfare Capability", *Defence Journal* (July 1998), www.defencejournal.com/july98/pakneeds1.htm

[22] Department of Defense, *Dictionary of Military and Associated Terms*, April 12, 2001.

[23] Jones, Kovacich and Luzwick, "Everything You Wanted to Know about Information Warfare but Were Afraid to Ask, Part 1", 9 -20.

[24] Stephen Blank, "Can Information Warfare Be Deterred?", *Defense Analysis* 17, no 2 (2001): 121-138, http://dx.doi.org/10.1080/07430170120064212 (accessed April 12, 2012).

[25] Ayers, "The New Threat: Information Warfare", 23-24.

[26] Ibid.

[27] Ibid.

[28] John Arquila and David Ronfeldt, "Cyberwar is Coming!", *Comparative Strategy* 12, no. 2 (Spring 1993): 141.

[29] Barrington M. Barrett Jr., "Information Warfare: China's Response to U.S. Technological Advantages", *International Journal of Intelligence and Counter Intelligence* 18, no. 4 (2005): 684-686, http://dx.doi.org/10.1080/08850600500177135 (accessed March 23, 2012).

[30] *Dictionary of Military and Associated Terms.*

[31] Barrett Jr., "Information Warfare: China's Response to U.S. Technological Advantages", 685.

[32] Wang Baocun, ''A preliminary Analysis of IW,'' *Zhongguo Junshi Kexue* (China Military Science), no. 4 (20 November 1997): 102–111; and Barrett Jr., "Information Warfare: China's Response to U.S. Technological Advantages", 685.

[33] Simson L. Garfinkel, "Inside Risks- The Cybersecurity Risk", *Viewpoints,* http://www.pccip.gov/, accessed on February 12, 2013; "President's Commission on Critical Infrastructure Protection", itlaw.wikia.com/.../President's_Commission_ on_Critical_Infrastructur..., accessed on February 12, 2013; and James Ellis (et) all, "Report to the President's Commission on Critical Infrastructure Protection", Special Report CMU/SEI-97-SR-003 , January 1997, www.cert.org/archive/pdf/97sr003.pdf, *accessed on February 12, 2013.*

[34] David J. Betz, "The More You Know, the Less you Understand: The Problem with Information Warfare", *Journal of Strategic Studies* 29, no. 3 (June 2006): 505-533, http://dx.doi.org/10.1080/01402390600765900, accessed on April 12, 2012.

[35] Cronin and Crawford, "Information Warfare: Its Application in Military and Civilian Contexts, 257-263; and Betz, "The more you know, the less you understand, 505-533.

[36] *Osgood, Encyclopedia of American Foreign Policy.*

[37] Jones, Kovacich and Luzwick, "Everything You Wanted to Know about Information Warfare but Were Afraid to Ask, Part 1", 9 -20.

[38] Ibid.

[39] Jonathan Reed Winkler, "Information Warfare in World War",*The Journal of Military History* 73, no. 3(July 2009); Report on March 29, 1918 cable cutting, 75, "U.K.-Verband, Kabelschneide- und Minenangelegenheiten, July 1917–August 1918"; The campaign against Allied communications is almost entirely unmentioned in standard accounts of World War I naval history by English-language authors, see, for example, Paul G. Halpern, *A Naval History of World War I* (Annapolis, Md.: Naval Institute Press, 1994).

[40] David Trask, *The War with Spain in 1898* (New York: Macmillan, 1981); Headrick, *Invisible Weapon,* 82–89; and Constantine Pleshakov, *The Tsar's Last Armada: The Epic Voyage to the Battle of Tsushima* (New York: Basic Books, 2003).

[41] Robert J. Bunker, "Battle space Dynamics, Information Warfare to Net war, and Bond-Relationship Targeting", *Small Wars & Insurgencies* 13, no. 2 (2002): 102, http://dx.doi.org/10.1080/09592310208559184.

[42] Lester W. Grau and Timothy L. Thomas, "A Russian View of Future War: Theory and Direction", *Journal of Slavic Military Studies* 9, no. 3 (1996): 501–518; Timothy L.Thomas, "Deterring Information Warfare: A New Strategic Challenge", *Parameters* 25, no. 4 (1996–97): 81–91; Timothy L. Thomas, "Russian Views on Information-Based Warfare", *Airpower Journal* (1996): 25–35; Edward Waitz, "The US Transition to Information Warfare", *Journal of Electronic Defense* (December 1998): 36; and Sergei Modestov, "The Possibilities for Mutual Deterrence: A Russian View", *Parameters* 26, no. 4 (1996–1997): 92–98.

[43] V. Men'vikov, I. Golovanev and S. Pavlov, "Soldiers of the Future*", National Air Intelligence Center*, July 1997, 3.

[44] Matthew Campbell, "'Logic Bomb' Arms Race Panics Russia", *The Sunday Times*, 29 November 1998; Stephen Blank, "Nuclear Strategy and Nuclear Proliferation in Russian Strategy", *Report of the Commission To Assess The Ballistic Missile Threat To The United States*, Appendix III, Unclassied Working Papers, Pursuant to Public Law 201, 1998, 57–77; and "Counter-proliferation in Russian Strategy" (paper presented to the JINSA-SSI Conference on Proliferation Strategies, Washington DC, 22 February 1999).

[45] Blank, "Nuclear Strategy and Nuclear Proliferation in Russian Strategy"; and Thomas, "A Russian View of Future War: Theory and Direction", 501-518.

[46] Stephenson, "Information Warfare, or, Help! The Sky Is Falling!", 6-10.

[47] "New war between India and Pakistan: Cyber Warfare", *Pakistan Defence*, February 8, 2011, www.defence.pk/.../122982-new-war-between-india-pakistan-cyber-warfare.html, accessed on April 9, 2012; Charles Billo and Welton Chang, "Cyber Warfare an Analysis of the means and Motivations of selected Nation States", *Institute For Security Technology Studies At Dartmouth College*, November 2004, www.ists.dartmouth.edu/docs/cyberwarfare.pdf, accessed on February 11, 2013, p.9; and S. M. Hali, "Cyber-warfare: New Arms Race", August 8, 2012, www.opinion-maker.org/.../cyber-warfare-new-arms-race/ (accessed February 11, 2013).

[48] Charles Billo and Welton Chang, "Cyber Warfare an Analysis of the means and Motivations of Selected Nation States".

[49] Shah, "Propaganda & Warfare in Cyber World".

[50] Ibid.; and Syed M. Amir Hussain, "Pakistan Needs an Information Warfare Capability", *Defence Journal*, July 1998, http://www.defencejournal.com/july98/pakneeds1.htm

[51] Farzana Shah, "Indo-Israeli Cyber Warfare against Pakistani Nuclear Program", *Asian Tribune*, September 9, 2009, http://www.asiantribune.com/.../indo-israeli-cyber-warfare-against-pakistani-nuclear-program (accessed April 10, 2012).

[52] Jones, Kovacich and Luzwick, "Everything You Wanted to Know about Information Warfare but Were Afraid to Ask, Part 1", 9 -20.

[53] Blank, "Can Information Warfare Be Deterred?", 121.

[54] Aashique Chaudhary, "Bollywood in Propaganda War against Pakistan", translation of an article from *Jang* (Rawalpindi), February 20, 2002, szh.20m.com/issues/bollywood.html (accessed March 17, 2012).

[55] Richard Sale, "U.S. Retains Hidden Grip on Pakistan's Nukes", *Pakistan Defence*, February 27, 2009, forum.pakistanidefence.com/index.php?showtopic=81170&mode..., February 28, 2009.

[56] Ibid.; "CIA's Drums Of War Against Pakistan", *Pakistan Defence*, May 17, 2011, www.pakistanideology.com/pakistan.../cias-drums-of-war-against-pakistan/, (accessed March 9, 2012).

[57] Shah, "Indo-Israeli Cyber Warfare against Pakistani Nuclear Program".

[58] Jawad Raza Khan, "Pakistan's Information War", *Pakistan ka khuda Hafiz*, May 17, 2011, www.pakistankakhudahafiz.com/2011/.../pakistan's-information-war/ (accessed April 9, 2012).

[59] Ibid.

[60] Ch Umar, "Propoganda Machine BBC Claims Pakistan's 'Support Taliban' – Western Propaganda Against Pakistan", 707monty.blogspot.com/.../bbc-secret-pakistan-biased-documentry.html, accessed on March 17, 2012; Sultan M Hali, "Hostile propaganda against Pakistan", *Pakistan Observer*, March 17, 2012, pakobserver.net/detailnews.asp?id=101867; and Abdul Zahoor Khan Marwat, "Propaganda against Pakistan mounts", *The News International* (Islamabad), May 11, 2011.

[61] "Propaganda of Indian RAW exposed in Balochistan" February 27, 2012, www.defenceblog.org/.../propaganda-of-indian-raw-exposed-in.html/,; and Marwat, "Propaganda against Pakistan mounts".

[62] "Propaganda of Indian RAW exposed in Balochistan". Pl link this reference with previous one

[63] Cronin and Crawford, "Information Warfare: Its Application in Military and Civilian Contexts".

[64] John Arquilla, "Can information warfare ever be just?"**,** *Ethics and Information Technology* (1999)**:** 203.

[65] E. Anders Eriksson, "Viewpoint: Information Warfare: Hype or reality?", 57.

[66] Hali, "Hostile propaganda against Pakistan".