LIBERAL STUDIES JOURNAL

LIBERAL STUDIES

A Bi-Annual Journal of School of Liberal Studies, PDPU, Gujarat

Vol. 1, Issue 1
January–June 2016

ISSN 2455-9857

EXPERTS SPEAK

ARTICLES

BOOK REVIEWS

Vol. 1, Issue 1 January–June 2016

SLS
SCHOOL OF LIBERAL STUDIES

Narottam Gaan*

Digital Age Security Threats: Challenges to IR Theories

The significance of information and communication technology (ICT) has been widely felt not only within a state but also among and between the states in their multifarious day-to-day interactions. Information and communication technology can be rightly said as constituting the nerve center of, both, domestic and international politics. These have become guiding metaphor for domestic and international politics to maintain stability and political order, provide peace and security and protect people from natural catastrophes. Sovereign state systems are no longer impregnable, sacrosanct; the unhindered flow of information and the revolutionary exposure of the people irrespective of which state, security or culture they belong to, to the very sinews of information, have made the entire world a melting pot of the absoluteness and arbitrariness of states. Earlier, issues confined to the boundary of the state or states have turned out to be global and mustered support from all sections, countries, nations and culture of the world. A new kind of threat from information and communication technologies seems to affect the states.

Some would argue walking on the conventionally trodden furrows that state is still the main player in international politics maintaining its supremacy in providing security even in cyberspace.[2] Others in a different vein maintain that the emergence of "virtual states" and network economies imply a decline of inter-state violence and hence the predominant role "security" playing in the past gets a plummeting. This optimistic undertone "sketches a future with an ever widening zone of international peace."[2] Still, there are many who hold that the information revolution has spurred many firms, interest organisations, social movements, individuals and transnational relations into

* The author is Professor (retd.), Department of Political Science, Utkal University, Odisha.

a network of activities and inter connections. Hence these non-state actors have become challengers to and providers of security.[3]

In other words, the general observation is that the information revolution has bunked the established notion that security is the unrivalled monopolistic concern of states only, and distance security away from state into an increasingly important concern of all sectors of society. Today all modern societies are information societies. Taking into account Arnold Wolfers definition of security as "the absence of threat to acquired values" it can be said that a threat to information services can be equally considered a threat to the acquired value of the society.

The challenges of information revolution for both security and its apparatus state remain unexplored in terms of policy and substantive issues. In the past no effort has been made to apply and develop theory on this topic. No serious efforts have been made to apply international relation (IR) theory in analysing the information revolution. It seems warranted to study the impact of information services on security and for development of international relation theory. John Eriksson and Giampiero Giacomello have made a commendable attempt at dovetailing the information revolution into the ambit of international relation.

During the post-WW II period, the discipline of IR was almost content with its Euro centric stance and putting on the Western straight jacket in analysing the events in the world it tried to look at with its own glass. It claimed universality and parsimony on the ground of the events in the world being understood on Western logic and idioms. This claim to universality and parsimony was at the expense of empirical applicability.[4] That means, the empirical applicability requires a greater degree of complexity and contextually contingent thinking than has been provided by the dominant international relation theories.[5] For example, theories such as Kenneth Waltz's neo-realism and Keohane and Nye's theory of complex interdependence were considered either irrelevant or secondary to claims of internal validity.[6] Utter discontentment with this inward looking obsession with theoretical consistency appeared on the scene with the demise of Cold War.[7] The end of Cold War signalled a major crisis for neo realism and IR theories for having failed to predict and explain the turn of events.

The Digital Age Literature Silent on the Security Issue

Marxist sociologist Manuel Castells was the fast proponent of the digital age. As early as the late 1980s, he noted that information had become the

primary resource of material productivity in the newly emerging "knowledge economy."[8] Information technology's influence was felt on banking, air travel, water, or energy distribution for their functioning. In the 1990s the network of information technology was all set to constitute an indispensable coping stone for modern and advanced societies. As pointed out by Castells, it was not long to see the dawn of global network society with nation states being stripped of their sovereignty and replaced by alternative identities and communities.[9]

He pointed to the perspective of transnational crime as will rise becoming the greatest potential threat to global security. Hamid Mowlana, another international scholar worked in a similar vein and agreed with Castells' analysis. But their study is limited to the impact of ICTs on organised crime,[10] military strategic communication and the use of information was propaganda.[11] According to Eriksson and Giacomello, Mowlana's work, though insightful, was weak in linking the information revolution to IR theory.

Control of Information by Governments to Preserve Sovereignty and Security

Before information revolution could affect the state, and reach out to the control of non-state actors, the main function to preserve national sovereignty and national security centered around the state's ability to control information flows.[12] The communication system was a one-way flow through radio and television from the national government to the entire people with its own monitored, cooked and controlled message. Increasingly in recent years, the state's stranglehold over information flows has slackened due to professional media organisations, human rights organisations, non-governmental organisations and individuals having taken advantage of the same communication system to exercise control over flow of information, produce counter claims, independent views and non-governmental information. The ingrained impregnability of state sovereignty seems to be made porous by the uninterrupted international flow of information from one corner to another. The entire nation has been exposed to the outside world and the inviolability of its sovereignty has been peeled off, layer by layer, by the flow of information to the outside world under its very nose. The international flow of information has been taking place so rapidly that the capability of states to control and monitor the ingoing and outgoing information is utterly compromised. This network of information flows transcending the traditional boundary of states has resulted in reinforcing an

integrated world communication system, which no longer remains captive to the control of state sovereignty.[13]

It is not that the importance of information was unknown to the states or the latter were not vulnerable to the assaulting power of the information. A report to the Swedish government, the Tengelin Report, also emphasised the main risks of a networked society including dependence on foreign vendors and the threat of hackers' raids.[14]

But, presently most governments are quite aware and even affected by the fact that the uncontrolled information flows transcending the territorial boundaries of states. This cross-county information flows and the easy accessibility of individuals to new channels and sources outside the country about its own political and economic structures, are very likely to affect the attitude of its own citizenry vis-a-vis its political and economic structure. When the states had control over its radio and TV channel and other free flow of information was not possible, when the information revolution was as its nascence, the extraordinary influence of information in forming the political attitude of the people *vis-a-vis* its state was subject to control and manoeuvrability. The difference is that what was once one-way traffic has now become multiple traffic with multiple entry points making the entire sovereign state system look like a porous pot and emasculating it to block the penetration of that information.[15]

What has changed the concept of security is the prominence that the global information society has given to ICTs in our thinking and approach to life. With the industrial revolution and invention of machines, human beings put machines in the centrality of their security. Machines could communicate with each other and become provider of security with more accuracy and precision at a faster rate than human beings could have been able to do in the past. With it also grows the psychological effect of fear and the dehumanising consequences of machines doing blunders. The solutions to societal problems were found in the machines. More than these machines, the development of computers could herald optimistic visions of technical solutions to societal problems or "technological fixes" as well as feelings of fear of these computers being turned evil.[16] Too much dependence on computers as the vital decision maker and sole arbiter of well-being and development of human beings has marked a drastic change in human society thinking and at the same time exposed human beings to the wrong or evil computers. Computers being masters of human destiny can escape into the hands of terrorists and evildoers to wreck havoc on humanity on a large scale than it could have been possible in the past. The entire world seems to be caught not in the network of

human relations, but in a network of communications. Subject to intrigue manipulation, computers through their electronic gadgets can create revolutionary psychological dimensions of network.

The most famous computer network, the Internet, is at the same time an infrastructure and a communication medium. "On the same wires and with the same protocol, packets transport bytes that represent radically different information: an email to a friend, details on one's flight itinerary, online multiplayer gaming, statistics on a municipality's water consumption, or credit card numbers."[17]

Most of the communication being public, anybody using the medium could read them. Earlier computer networks were proprietary linking together a bank with its subsidiaries or US strategic command with nuclear missile silos was too expensive to be afforded by other organisations and institutions. Further, they used protocols that authorised their legitimate users to be in the network. Today the cost of networking has been comparatively less expensive and easily affordable with availability of multiple channels and unobstructed accessibility. The network of communication has been very simple making everybody nude. What was unnoticed, unwanted, undesirable or improper to intrude, has now become public. When man was the master and sole communicator the security of communication was fully insulated from others' intrusion. Today, Internet easily passing into every hand has taken away the security of communication at a higher price of providing sinews and opportunities to criminals and evil mongers to exploit the vulnerabilities of the network for their own narrow interest.

Cyber Threats in the Post Cold War Security Thinking: A Theoretical Understanding

The end of Cold War marked remarkably a downsize in the budgetary allocation for defense and military establishment. A shift of focus on conventional warfare to information security and cyber threats was perceived. Allusion to buzzwords like critical information, protection, information warfare, information operations, information assurance, cyber terrorism and Revolution in Military Affairs (RMA) became common among the analyst and policy maker in defense and military establishments.

The increased vulnerability of individuals, people, security and states to information resolution and loss of control over it has given rise to a fear resulting in what is termed as cyber threat. This has been owing to the transformation of industrial society into an information society.[18]

Images of cyber threats are found dominating in both public and private spheres, among both military as well as civilian actors. These became rampant with the world coming under the global computer network and communication. In the business community and within police, cyber crime has become a salient threat image.

With the bureaucratic-military establishment, perceived threats have been framed as information warfare, information operation, cyber terrorism and cyber war. Both state and non-state actors can come within the targets and adversaries of image of cyber threats.[19]

According to Eriksson and Giacomello, "states are still typically seen as the single most important type of potential enemy, able to neutralise effectively the critical infrastructure of another country."[20]

There is no dearth of literature to show the theoretical dramatisation of the potential cyber threats and information security. A study by the National Research Council argues that "Tomorrow's terrorist may be able to do more with a keyboard than with a bomb."[21] Former US Homeland Security Director Tom Ridge (2002) observed that "Terrorists can sit at one computer connected to one network and can create world havoc – [they] do not necessarily need bombs or explosive to cripple a sector of the economy or shut down a power grid." The view doing the round is that the governments and societies are becoming more dependent on and comfortable with information technology, but at the same time are becoming increasingly vulnerable to all sorts of cyber threats being dramatised theoretically. The glaring example of cyber threats being theoretically dramatised is the electronic Pearl Harbor.[22]

It is a dramatised apocalyptic vision of a situation where all governments' critical infrastructures and foundations totally depending on information technology would come to a grinding halt. Banks, phone system, subway cars would come to a standstill putting thousands of people in jeopardy. This became the cynosure of many newspapers and media in the US, and its policy makers in certain circles started working on this. Former Deputy Defense Minister John Hamre argued that "we are facing the possibility of an electronic Pearl Harbor…There is going to be an electronic attack on this country sometime in the future."[23]

But, there are critics who jibe at such rhetorical dramatisation of potential cyber threats, castigating these as highly unlikely. Denning (2001 b) argues that cyber terrorism, defined as digital attacks, causing physical destruction and human deaths is extremely unlikely. Even the US Naval War College in

cooperation with the Gartner Group concluded that an "electronic Pearl Harbor", although theoretically possible was highly unlikely: "These are far simpler and less costly ways to attack critical infrastructure, from hoax phone calls to track bombs and hijacked airliners."[24]

The major impact of information operations is the symbolic and the main effect is humiliation. Operating with online transactions, the firms incur a heavy financial loss. To a large degree cyber attacks are attacks with and against symbol and images. Denial of service attacks and the defacing of web pages certainly can have material consequences.

According to some analyst, the cyber attacks have been mostly transnational and network based.[25] Adversaries can be termed as network actors consisting of relatively independent nodes of individuals, groups, organisations or even states capable of quickly assembling and dispersing, even long before an attack has been discovered. These actors operating in loosely organised networks and using such means can resort to asymmetric warfare.[26] These warfares may not be conventional military conflicts, but are capable of wreaking serious damages by attacking and exploiting the vulnerabilities of information system by resorting to cyber attacks.[27]

The conventional understanding of sovereign state system is premised on boundary making and spatial distancing. With the prospect of cyber attacks and information security the boundaries fencing off states against the other, demarcating the international sphere from the domestic sphere, the public from the private, peace from war and the military from the civil, are dissolved. One of the major implications of cyber threats is that the security of the information system on which the entire network of organisation, individuals, groups and even states hinges, is challenged. Besides, the very impregnability and invincibility of sovereign state system is challenged.[28] The very foundation of sovereign state system that it is solely capable of serving control of the national territory and the people residing within it, is shaken. External sovereignty is also at stake due to easy accessibility to computer networks of all for manipulation and exploitation.

Security Studies Silent about Information Security

Security studies resolve basically around two contending positions – traditionalists and the wideners. The traditionalists hold on to their ingrained stance that security is basically state-centric and military-oriented. Despite cataclysmic changes in the international realm in terms of the end of Cold War, growing spate of ethnic and religious insurgence, global terrorism,

transnational crime and global warming, their age-long stance on state-centric security has not changed because of their preference for theoretical clarity and coherence.[29]

The wideners in contrast to the traditionalists claim that the concept of security should be widened to include within its ambit the new challenges, threats emanating not only from other states, but from the political, societal, economic and environmental sectors.[30] Whereas in the traditionalists' view state was the center piece of security, in the widener's view state is not the only linchpin of security concern, there are other non-state actors like NGOs, social movements, terrorist organisations, private firms and individuals who pretend status equally with states in the security concerns. The traditionalists' focus is on the state, but distancing away from the state the wideners focus on individual under the rubric 'human security'. What is surprising is that in their broadened perspective no attention has been paid to the information revolution and its impact on security. While their concept of widened security incorporates everything spanning political, electronic, ecological and cultural issues, it rarely addresses the emergence of Internet and information revolution and their impact on security. On the other hand, some traditionalists have tended to give importance to development of information technology to the extent it has been of immense utility to improvement of military capabilities.[31]

Enhancement of material capabilities has always been considered crucial to state-centric and military-oriented national security. Intelligence gathering and psychological warfare (a play of information operations) are also considered as elements of material capabilities of states and intrigue parts of warfare. The military and material aspects of states have evinced a greater interest in technological and information revolution as these would enhance their military capability and modernise the technology of warfare. The passage of state military apparatus from machine guns to radar and satellites demonstrates the interest traditionalists have shown in the utility of information technology to the enhancement and modernisation of military capability of states. 'Electronic warfare' has been an established practice and concept within the military for several decades. But most traditionalists while sticking to their conventionally held stand on state-centric security are of the view that "information technologies are merely a new fancy add on."[32]

Relevance of Information Security from the Perspective of Major IR Theories on Security

The contemporary international relations is mainly dominated by three theoretical perspectives –realism, liberalism and constructivism, which are

perceived and portrayed as separate perspectives, though these have linkages, overlaps and internal varieties. In the light of the digital age and information revolution, the relevance of each perspective can be examined.

Realism

Despite information revolution in the digital age, realists have preferred to cling to their main thesis that state is the sole and main actor in both domestic and world politics with primacy on military power and process, denying the non-state actors any power to play along with state. They would like to face the challenges of the information revolution in much the same way as they have tackled previous challenges of transnationalisation, complex interdependence and globalisation. These challenges may affect the policies of domestic politics and structure of the state but would not any way undermine the primacy of state as the supreme political unit and change their ingrained view about the anarchic international system.

The realist would like to treat the ICT related security threats as coming under the rubric of economic issue not as security threats in themselves to penetrate into bastion of impregnability of states. There are some realistic still inclined to define a narrow military-centric definition of security, and believe that if widening of the concept of security is warranted, then it should incorporate the economic dimension without compromising its primacy.[33] Interestingly, they try to understand the new information warfare as new and digressing away from state but as a component in otherwise traditional interstate conflict.[34]

The case of electronic warfare such as the jamming of radio communication since the WW II for a much shorter time has been an element of inter-state conflict. To realists this is not threat, it is rather a change in the warfare within the state military apparatus presaging the greater change in the digital age warfare, which comes within the military apparatus of state as a part of its modernisation process. The realists view the introduction of information warfare in strategic studies and military planning as a part of its modernisation process. The realists view the introduction of information warfare in strategic studies and military planning as a continuation of its traditional military thinking, not as a dramatic change envisaging the overhaul of the state centric security paradigm. The information revolution may have introduced new technologies into the warfare with new digital adversaries, "but the basic notion of attacking at defending information systems are as old as warfare itself- basically old wine in new bottles."[35]

Liberalism

Rejecting the realist view as one-sided and normally focused, the sociological liberalism holds that international relation is not only about state-state relation, it is also about transnational relations, that is relation between people, groups and organisations belonging to different countries. State is not the only actor, there are plurality of non-state actors. Transnational relations are considered by sociological liberals to be an increasingly important aspect of international relation. According to Rosenau, trans-nationalism marks "the process whereby international relations conducted by governments have been supplemented by relations among private individuals, groups and societies that can and do have important consequence for the course of events."[36] In a similar vein, Karl Deutsch argued that a high degree of transnational ties between societies leads to peaceful relations that amounts to what is called 'security community'.[37] John Burton in his book, *World Society* (1972), purposes a 'cobweb model' of transnational relationships among different groups of people – religions, business, labour, with different types of external ties and different types of interests.

Rosenau studies transnational relation at the macro-level of human population coupled with those conducted at the micro-level by individuals. Perceiving a profound transformation of the international system, he is of the view that the state-centric anarchic system has not disappeared but a new multi-centric world has emerged that is composed of diverse "sovereignty free" collectivities, which exist apart from and in competition with the state-centric world of sovereignty-bound actors.[38]

Interdependence liberalism is of the view that modernisation increases the level and scope of interdependence between states. Under complex interdependence, transnational actors are increasingly important, military force is a less useful instrument, and welfare –not security-is becoming the primary goal and concern of states. According to Rosecrance, the end of Cold War has made the traditional option less urgent and thus less attractive. Consequently, the trading-state option is increasingly preferred even by very large states. David Mitrany (1960) put forth a functionalist theory of integration arguing that greater interdependence in the form of transnational ties between countries could lead to peace. Built on Mitrany's functionalism but rejecting his separation of technical experts from politicians, Ernst Haas enunciated the doctrine of neo-functionalist theory of international integration which is a process whereby "political actors are persuaded to shift their loyalties toward a new center where institution possesses or demands jurisdiction over the preexisting national states.[39]

Robert Keohane and Joseph Nye, *Power and Interdependence* (1977), propounded a general theory of what they called "complex interdependence", which is qualitatively different from earlier and simpler kinds of interdependence.[40] Under conditions of complex interdependence relations between states nowadays, or even primarily relations between state leaders, there are relations on many different levels via different actors and branches of government between individuals and groups outside of the state. Further, military force is a less useful instrument of policy under conditions of complex interdependence. In the words of Nye:

> The appropriate response to the changes occurring in world politics today is not to discredit the traditional wisdom of realism and its concern for the military balance of power, but to realise its limitation and to supplement it with insights from the liberal approach."[41]

Institutional liberals differ from realists in that international institutions are mere scraps of paper and that they remain always hostage to the powerful states. International institutions are always of interdependent importance promoting cooperation between states.[42]

One way to assess the institutional liberal view is to set it against that of neo-realist analysis. Neo-realists argue that the end of Cold War is likely to bring the return of instability. But the institutional liberals (Keohane, Nye, Keohane) are of the view that a high level of institutionalisation significantly reduces the destabilising effects of multi-polar anarchy identified by Mearsheimer.[43] While promoting cooperation between states, institutional liberalism can help alleviate the lack of trust between states and states' fear of each other, which are considered to be the traditional problems associated with international anarchy.

Having with it the normative element the Republican Liberalism advocates that democracies do not go to war against each other owing to their domestic culture of peaceful conflict resolution, their common moral values, and their mutually beneficial ties of economic cooperation and interdependence.[44]

To sum up this, it can be said that the development of increasingly complex and globally penetrating web of transnational relations and emergence of non-state actors has challenged the political and economic stranglehold of the state and made it pregnable against the perforating penetration of transnational relations.

With shift of emphasis on state to other non-state actors and other transnational relations, liberalism has broadened the definition of what international relations is about, and regarded economics as much important

as security. As a result, some liberals advocated a widened perspective of security, which includes economic, ecological and human security concerns. Joseph Nye and Robert Keohane, the advocates of theory of complex interdependence in the 1970s, have recently updated this to meet the challenges of the digital age.[45] While treating the costs of interdependence in terms of vulnerability and sensitivity as new component of the theory and frame them purely in economic terms not portrayed as matters of national and international security, they have analysed the impact of information revolution on international relations.[46]

Nye is of the view that national security defined as the absence of threat to major values can be at stake. Within his theoretical framework is found absence of any elaborated analysis of critique of cyber security threats. Nonetheless, his concept of 'soft power' can be of relevance to this topic. Soft power is the "ability to get what you want through attraction rather than coercion or payments. It arises from the attractiveness of a country's culture, political ideals, and policies…. Soft power rests on the ability to shape the performance of others."[47] Thus, modern liberalism seems to be greatly influenced by Kantian and Wilsonian idealism.[48] Nye wants these ideals to spread to other parts of the globe, through the exercise of soft power. In his view, relevance of soft power is more highlighted than ever in this digital age because of the ever increasing evolution of multiple channels of global communication transcending the sovereign boundaries.[49] It would be a mistake to imagine that the soft power and global ICTs that facilitate the opening of multiple channels of communication and interaction are only instruments of cooperation, democratisation and peace, as Nye and other liberals would like to believe. These channels may be exactly the opposite instruments of deception, propaganda, threats and terror.

Casting aside its idealism and fear of treading on realist furrow of security analysis, liberalism could be said to be throwing insights into the nature of security threats in the digital age. In particular, this view is sustained and reinforced by the attention that the liberals pay to the growing emergence of non-state sovereignty free actors and the global complex interdependence in costs in terms of vulnerability and sensitivity. Eriksson and Giacomello cite two socio-economic trends that are found consistent with the dictum of liberal theory:

(1) expanding partnership between the public and private sector to provide services;

(2) merging of the civil and military spheres.[50]

The very recognition of their growing incapability to meet the burgeoning demands of the modern societies has led the governments to promote public-private partnership. The trends of privatisation in the age of market economy quite evident in the sectors of health, education, transport and other services have been extended to national security. For example, in the United States, the National Strategy to secure cyberspace of the President's Critical Infrastructure Protection Board of September 2002 relies on public-private partnership, conceding that "Government alone cannot secure cyberspace."[51] This has resulted in what is called civilianisation of the military or, perhaps, militarisation of the society."[52]

No sector is most apparently permeated by this integration and complex interdependence than the telecom sector. It has always been the practice with the military to use the help of civilian telecom networks. Nowadays the dependence of vast majority of military communication on civilian networks for transmission has been profusely vast. Computer networks have been incorporated into the development of hard military powers and have formed the foundation of soft power.[53]

It needs a critical analysis of the question whether a theory that was originally crafted to study actors and process in a political-economy context, can dovetail the impact of information revolution in a digital age into their theory. The question still remains unanswered whether the development of the ICTs in the age of globalisation and modernisation is a continuation of the process of transnationalisation and complex web of interdependence.

Nevertheless, cyber threats and challenges of information revolution representing the current trends of development in the age of globalisation appear to emasculate the sovereignty and security of the states. The non-state actors are numerically spawning and becoming powerful as found from their active participation and involvement in various domestic and international issues, because of information revolution. The emergence of Internet and network of communications and interaction with online groups may have facilitated integration, cooperation and liberation transcending the barricades of state sovereignty from a positive perspective, but certainly have brightened the prospect of terrorism, transnational crime and the destabilisation of states.

The very recognition that beside state there are a plurality of non-state actors is the very valuable contribution by liberalism to theory building with regard to security in the digital age. But this still remains underdeveloped.

Arquilla and Ronfeldt are among the few scholars who also study mainstream liberal notion of globalisation and other challenges to state sovereignty and address explicitly the issue of actor plurality in the digital age.[54]

Constructivism

Rejecting the one-sided material focus of realists, constructivists argue that the most important aspect of international relations is social, not material. In their views, the social reality is not objective or external. The social and political world including the world of international relations is not a physical entity or material object that is independent of human consciousness. Consequently, the study of IR must focus on the ideas and beliefs that inform the actors on the international scene as well as the shared understandings between them.

Liberalism basically founded and on neo-realist assumptions as starting point is vulnerable to the diatribes directed against neo-realism by constructivists. After the end of the Cold War some liberals began to focus on the role of ideas. Fukuyama's *End of History* (1989) focused on the role of the ideas in spreading democratic and liberal values to all parts of the globe. Even if constructivists are sympathetic to several elements of liberal thinking, their focus is less on advance of liberal ideas, than on the role of thinking and ideas in general.

Constructivists maintain that the social world is in part constructed by physical entities or material reality. But it is the ideas and beliefs concerning those entities which are most important. The international system of security and defense, for example, consists of territories, populations, weapons and other physical assets, computers, ICTs and communication channels that could also be included within its ambit. But it is the ideas and understandings according to which those assets are conceived, organised and used that is most important. This could be termed social reality. "The thought that is involved in international security is more important, far more important than the physical assets that are involved because those assets have no meaning without the intellectual component: they are mere things in themselves."[55] To quote Wendt: "The claim is not that ideas are more important than power and interest, or that they are autonomous from power and interests. The claim is rather that power and interests have the effects they do in virtue of the ideas that make them up."[56]

Constructivism does not take a general stance as to what can be or cannot be framed as a security threat and how such threat can be dealt with. It focuses

on the verb "become rather than can or cannot";[57] constructivist security studies emphasises on identity and culturally related threats, which are downplayed in realist and liberal accounts of security.[58] The empirical amenability of constructivism to the widest possible range of perceived security threats makes it possible to address all kinds of threats. "In terms of threats to critical infrastructures, this would, for example, include not only digital attacks, but also technical collapses and bugs such as the infamous Y2K problem, as well as natural disasters such as earthquakes and violent eruption."[59]

The constructive approach to security is the theory of "securitisation" developed by the Copenhagen School. This is about how, when and with what consequences political actors construct something as a matter of security.[60] The emphasis is on speech acts i.e. political language and the implication this has for political agenda setting and political relations. Securitisation implies that an "existential threat" is identified, and the "speech act" prioritises the issue on the political agenda, legitimating extraordinary measures such as secrecy, the use of force and the invasion of privacy. But on its advocacy of widening of security agenda, the Copenhagen School has lost sight of the information revolution.

Eriksson has pioneered the study of securitisation of information technology in Swadeshi politics. His analysis demonstrates the impact of different frame of IT related threats on whom or what is blamed, and who is allocated responsibility for dealing with the problems.[61] Framing an incident as "cybercrime" implies that criminals are to be blamed, and that the police are responsible for dealing with them. In contrast, the same incident can also be framed as an instance of 'information warfare' which implies that enemies to a given nation state, other states or non state actors are to be blamed, and that the military has a responsibility to respond to the threat.[62]

In the current analysis of digital security threats the constructivists put emphasis on how information warfare challenges a multitude of boundaries, notably boundaries of identity. Everard (2000) argues that information warfare is a particular kind of "identity warfare" in which all kind of boundaries are challenged, including the classical domestic international divide. Hence the identity of nation state is always threatened, although it may adapt to the constant penetration into the sovereign state by cyber threats, and to the emergence and articulation of new identities in cyber space.[63]

In addition to material reality of computers and cables, the significance of images and symbols finds a peremptory place in the constructive analysis

of power and security in a virtual world. Distancing of actors from the bloody war has been one of the many effects of war in the digital age.[64]

Due to Internet and Information Revolution from anywhere in the world, a computer can be attacked in distant places of the world. Having said this, it does not in any way undermine the significance of decreasing geographical distance. What is significant here is how virtuality affects the conduct and perception of the war. Digital war is akin to computer games to the extent that simulation is performed and perceived in the same way by using the mouse and keyboard of a computer. The boundary between the real and imagined is thus blurred. What is important here is to note that the film, tabloid and computer gaming industries with their effects, tactical tools and software have become an increasingly important source of inspiration and expertise for the military.[65]

The use and abuse of symbols for manipulating political discourse and public opinion known as symbolic politics has assumed significance for studying digital age security. Long before the information revolution came into the picture, the symbolic politics of approach for the first time laid by Murray Edelman could be held as a constructivist contribution in social science.[66]

Defacing websites, a noteworthy practice of symbolic politics can be compared to the burning of an enemy's flag. What is important here is not the negligible cost involved in mending a website and securing a server; the cost in terms of lost confidence, disparagement and feeling of vulnerability, however, is immense. Assaults and counter attacks against USA and Chinese Government websites by hackers from the respective countries are very much in the news. Similar digital wars are going on between Israeli and Arab hackers and between Indian and Pakistani ones. This symbolic politics approach, much practiced in computers, smacks of how and why these actions are seen as an insult and offense to national pride. The Internet has become the new global battlefield for symbolic politics.

The function and impact of language in digital age security has been illustrated by the constructivist analysis. Frequent reference to bugs, viruses, worms and fire walls in computer with analogies to things familiar in the real or off-line world has rendered the abstract and technically complex world of cyber security intelligible.[67] Although the information warfare and electronic Pearl Harbor are constantly referred to as digital by nature, it has nonetheless physical consequences equal to those of conventional war. Constructivist

analysis can play a significant role in revealing and understanding the importance of rhetoric and symbolic actions in politics. Eriksson and Giacomello have very succinctly attempted to demonstrate the need to develop middle range theories integrating liberalism, constructivism and realism for comprehending the impact of information revolution on security.

Conclusion

As found out from the above analysis of various theories on security, short shrift has been paid to the security problems of the digital age by the scholars. Realism persists with its entrenched habit of putting emphasis on state and its military apparatus. On the other hand, liberalism and constructivism have widened the base of security and made a discursive approach to security. Liberalism denuded of its idealist and anti-realist pretensions entails within it many of the elements of the security in the digital age. The advocacy of multiplicity of non-state actors with transnational capacity, network economics, vulnerability, interdependence and consequent perforation of formally sovereign boundaries have enabled it to grasp the impact of information revolution on security. In a similar vein, constructivism has analysed the symbolic, rhetorical and identity based aspects of digital age security. Realism has tried to understand the impact of information revolution and digital age security by subsuming it under state as it was wont to understanding globalisation and other challenges by relating it to political economy or domestic politics under the rubric "state."

Even in the classical realist formulation of security, information warfare is merely held as the technological continuation of classical forms of psychological warfare and more recently of electronic warfare. In this classical perspective the developments in the information technology in the digital age are seen as nothing but an unfolding of technological change in the military warfare within a military-centric state. The foregoing analysis demonstrates how the IR theories on security are plagued by the dichotomy between theory and practice in the digital age. All current theories are inherently weak so far as the theoretical adoption and application in analysis of the complexities of the emerging information revolution in the digital world are concerned. Therefore, adoption of a pragmatic approach founded on bridging the gap between theory and practice by taking insights from methodological pluralism and theoretical complementarities seems warranted to incorporate digital security into the corpus of IR theories.

Notes

1. J.E. Fountain, *Building the Virtual State: Information Technology and Institutional Change*, Washington, DC: Brookings Institution, 2001.
2. R.N. Rosecrance, *The Rise of the Virtual State: Wealth and Power in the Coming Century*, New York: Basic Books, 1999, p. 24.
3. J. Arquilla and D. Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica, CA: RAND, 2001.
4. C. Wight, "Philosophy of Social Science and International Relations", in W. Carlsnaes, T. Risse, and B.A. Simmons, eds., *Handbook of International Relations*, London: Sage Publications, 2002.
5. A. George and A. Bennet, *Case Studies and Theory Development in the Social Sciences Cambridge*, MA and London: MIT Press, 2005.
6. R. Keohone and J.S. Nye, *Power and Interdependence, World Politics in Transition*, Boston, MA: Little Brown, 1977, p. vi; K.N. Waltz, *Theory of International Politics*, New York: McGraw Hill, 1979, pp. 6–7; C. Wight, "Philosophy of Social Science and International Relations", in Carlsnaes, et al., n. 4.
7. P. Allan, K. Goldmann, eds., *The End of the Cold War: Evaluating Theories of International Relations*, The Hague: Kluwer Law International, 1995; R.N. Lebow, Raise, and T Kappen, *International Relations and the End of the Cold War*, New York: Columbia University Press, 1995.
8. M. Castells, *The International City: Information Technology, Economic Restructuring, and the Urban-Regional Process*, Oxford: Blackwell, 1989.
9. M. Castells, *The Information Age: Economy, Society and Culture*; vol. 1: *The Rise of the Network Society*, Malden, MA: Blackwell, 1996; Castells, vol. 2: *The Power of Identity*, Malden, MA: Blackwell, 1997; Castells, vol. 3: *End of Millennium*, Malden, MA: Blackwell, 1998.
10. *Ibid.*
11. H Mowlane, *Global Information and World Communication, New Frontiers in International Relations*, London, Sage, 1997.
12. J. Agnew, S. Corbrige, Mastering Space: Hegemony, Territory and International Political Economy, London: Routledge, 1995; C. Anderson, "The Accidental Superhighway. A Survey of the Internet," *The Economist*, 01 July 1995; S Krasner, "Power Politics, Institution and Transnational Relations" in T. Risse Kappen, ed., *Bringing Transnational Relations Back In*, Cambridge: Cambridge University Press, 1995.
13. J.A Camilleri, J. Falk, *The End of Sovereignty: The Politics of a Shrinking and Fragmenting World*, Aldershot: Edward Elgar, 1992.
14. V. Tengelin, "The Vulnerability of the Computerised Society," in H. Gassmann, ed., *Information, Computer and Communication Policies for the '80s*, Amsterdam: North Holland Publishing Company, 1981.
15. Eriksson Johan and Giampiero Giacomello, "The Information Revolution, Security, and International Relations Relevant Theory", *International Political Science Review*, vol. 27, no.3, July 2006, p. 244.

16. R. Volti, *Society and Technological Change*, 3rd edn. London: St. Martin's Press, 1995.
17. Eriksson and Giacomello, n. 15, p. 225.
18. D. Alberts, *The Unintended Consequences of Information Age Technologies*, Washington, DC: National Defense University, 1996; Alberts, *Defensive Information Warfare*, Washington, DC: National Defense University, 1996; D Alberts and D. Papp, eds., *The Information Age: An Anthology on Its Impacts and Consequences*, Washington, DC: National Defense University, 1997; R. Henry and C.E. Peartree, eds., *The Information Revolution and International Security*, Washington DC. Center for Strategic and Inter-national Studies, 1998; A O'Day, ed., Cyberterrorism, Aldershot: Ashgate, 2004.
19. O'Day, ibid; D. Polikanov, ed., *Information Challenges to National and International Security*, Moscow: PIR Center, 2001.
20. Eriksson and Giacomello, n. 15, p. 226.
21. R. Bendrath, "The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection," *Information and Security*, no. 7, 2001, pp. 80-103; DE Denning, "Activism, Hacktivism, and Cyberterrorism, The Internet as a Tool for Influencing Foreign Policy," in J. Arquilla and J. Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime and Militancy*, Santa Monica, CA: RAND, 2001, p. 282.
22. J. Everard, *Virtual States: The Internet and the Boundaries of the Nation-State*, London: Routledge, 2000; R. Forno, Quotes on "Electronic Pearl Harbor," 25 July 2002, URL: http://www.soci.niu.edu/~crypt/other/harbor.htm; G. Smith, "An Electronic Pearl Harbor? Not Likely," *Issues in Science and Technology*, 1998, URL: http://205.130.85.236/issues/15.1/smith.htm
23. CNN, "Experts Prepare for an 'Electronic Harbor,'" 07 November 1997, URL: http://www.cnn.com/US/9711/07/terrorism,infrastructure
24. *The Economist*, 2002, p. 19.
25. R. Deibert and J.G. Stein, "Social and Electronic Networks in the War on Terror" in R. Latham, eds., *Bombs and Bandwidth: The Emerging Relationship Between IT and Security*, New York: New Press, 2003; J. Arquilla and D. Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy*, Santa Monica, CA: RAND, 1999; Arquilla and Ronfeldt, n. 21.
26. M Applegate, *Preparing for Asymmetry: As Seen Through The Lens of Joint Vision 2020*, Carlisle: Strategic Studies Institute, 2001; Arquilla and Ronfeldt, n. 21; A.D. Sofear and S.E. Goodman, *The Transnational Dimension of Cyber Crime and Terrorism*, Stanford, CA: Hoover Institution Press, 2001; G.P. Herd, "The Counter-Terrorist Operation in Chechnya: Information Warfare Aspect", *Journal of Slavic Military Studies*, vol. 13, no. 4, 2000, pp. 57–84; M. Erbschloe, *Information Warfare: How to Survive Cyber Attacks*, Berkeley, CA: Osborne and McGraw Hill, 2001.
27. Arquilla and Ronfeldt, 1999, 2001, n. 21; A. Cordesman, *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection Defending the US Homeland*, Westport, CT: Praeger, 2002.

28. J. Everard, *Virtual States: The Internet and the Boundaries of the Nation-State*, London: Routledge, 2000; Fountain, 2001, n. 1; G. Giacomello, *National Governments and Control of the Internet: A Digital Challenge,* London: Routledge, 2005.
29. M. Ayoob, "Defining Security: A Subaltern Realist Perspective", in K. Krause and M.C. Williams, eds., *Critical Security Studies: Concepts and Cases*, London: UCL Press, 1997; K. Goldmann, "Issues, Not labels, Please! Response to Eriksson", *Cooperation and Conflict*, vol. 34, no. 3, 1999, pp. 331–3.
30. B. Buzan, *Peoples, States and Fear: An Agenda for International Security Studies in the Post Cold War Era*, 2nd edn., Boulder, CO: Lynne Rienner, 1991; H. Muller, "Security Cooperation" in W. Carlsnaes, T. Risse and B.A. Simmons, eds., *Handbook of International Relations*, London: Sage Publications, 2002; E. Stern, "The Case for Comprehensive Security," in D. Deudney and R. Matthew, eds., *Contested Grounds: Security and Conflict in the New Environmental Politics*, Albany: State University of New York Press, 1999.
31. D.J. Lonsdale, "Information Power: Strategy, Geopolitics, and Fifth Dimension", *Journal of Strategic Studies*, vol. 22, no. 2–3, 1999, pp. 137–57.
32. Eriksson and Giacomello, n. 20, p. 228.
33. Buzan, n. 30; S. Walt, "The Renaissance of Security Studies," *International Studies Quarterly*, vol. 35, no. 2, 1994, pp. 211–39.
34. D.J. Lonsdale, "Information Power: Strategy, Geopolitics, and Fifth Dimension", *Journal of Strategic Studies*, vol. 22, no. 2–3, 1999, pp. 137–57.
35. Eriksson and Giacomello, n. 15, p. 229.
36. J.N. Rosenau, *Turbulence in World Politics: A Theory of Change and Continuity,* Princeton, NJ: Princeton University Press, 1990, p.1.
37. K.W. Deutsch, et al., *Political Community and the North Atlantic Area*, Princeton: Princeton University Press, 1957.
38. J.N. Rosenau, *Turbulence in World Politics: A Theory of Change and Continuity,* New York Harvester Wheatsheaf, 1990, p. 282.
39. E.B. Haas, *The Uniting of Europe: Political, Socia and Economic Forces (1950-1957),* Stanford: Stanford University Press, 1958, p. 16.
40. R. Keohone and J.S. Nye, *Power and Interdependence, World Politics in Transition*, Boston, MA: Little Brown, 1977.
41. J.S. Nye Jr, *Bound to Lead: The Changing Nature of American Power,* New York: Basic, 1990, p. 177.
42. M.A. Levy, O.R Young and M. Zurn, "The Study of International Regimes", European Journal of International Relations 1/3, 1995, pp. 267–330; O.R. Young, International Cooperation: Building Regimes for Natural Resources and the Environment, Ithaca: Cornell University Press, 1989; V. Rittenberger, ed., Regime Theory and International Relations, Oxford: Clarendon Press, 1993.
43. J. Mearsheimer, "Back to the Future: Instability in Europe after the Cold War", in S. Lynn Jones, ed., *The Cold War After: Prospects for Peace*, Cambridge, MIT Press, 1993, pp. 141–92.

44. G. Sorensen, "Kant and Process of Democratisation: Consequences for Neo-realist Thought", *Journal of Peace Research*, vol. 29, no. 4, 1992, pp. 397–414; C. Lipson, *Reliable Partners. How Democracies Have Made a Separate Peace*, Princeton: Princeton University Press, 2003; Adler Emanuel and Michel J Barnett, "Governing Anarchy: A Research Agenda for the Study of Security Communities," *Ethics and International Affairs*, vol. 10, 1996, pp. 63–98; W.R. Thompson, "Democracy and Peace: Putting the Cart before the Horse?," *International Organisation*, vol. 50, no. 1, 1996, pp. 141–75.
45. R Keohane and J.S. Nye, "Power and Interdependence in the Information Age," *Foreign Affairs*, vol. 77, no. 5, 1998, pp. 81–94; J.S. Nye, Jr., *Under-standing International Conflicts: An Introduction to Theory and History*, 4th edn., New York: Pearson and Addison Wesley, 2003; Nye, *Power in the Global Information Age: From Realism to Globalisation*, London: Routledge, 2004.
46. Nye, ibid.
47. J.S. Nye, Jr., "Soft Power: The Means to Success in World Politics", *Public Affairs*, New York, 2004, pp. x, 5.
48. R.W. Duncan, B. Jancar-Webster, and B. Switky, *World Politics in the 21st Century*, New York: Longman, 2003, pp. 21–22, 32–34.
49. Nye, n. 45, Chapter 7.
50. Eriksson and Giaconello, n. 15, p. 231.
51. PCCIP, "Fact Sheet, President's Commission on Critical Infrastructure Protection, 2000, URL: http//www.info-sec.com/pccip/web/backgrd.html
52. Eriksson and Giaconello, n. 15, p. 231.
53. Fountain, 2001, n. 1; Nye, *The Paradox of American Power: Why the World's Only Superpower Can't Go It Alon*e, Oxford: Oxford University Press, 2002; Nye, "Soft Power: The Means to Success in World Politics", New York, *Public Affairs*, 2004.
54. Arquilla and Ronfeldt, 2001, n. 3.
55. Robert Jakson and Georg Sorensen, *Introduction to International Relations: Theories and Approaches*, (Indian edition), Oxford University Press, 2008, p. 165.
56. A. Wendt, *Social Theory of International Politics*, Cambridge: Cambridge University Press, 1999, pp. 135–6.
57. E. Adler, "Constructivism and International Relations," in W. Carlsnaes, T. Risse and B.A. Simmons, eds., *Handbook of International Relations*, London: Sage Publications, 2002, p. 95.
58. B. Buzan, O. Waever and J. De Wilde, *Security: A New Framework for Analysis*, Boulder, CO: Lynne Rienner, 1998.
59. Eriksson and Giacomello, n. 15, p. 234.
60. Buzan et al, 1998, n. 58; O. Waever, "Securitisation and Desecuritisation," in R.D. Lipshutz. ed., *On Security*, New York: Columbia University Press, 1995; M.C. Williams, "Words, Images, Enemies: Securitisation and International Politics," *International Studies Quarterly*, vol. 47, no. 4, 2003, pp. 511–31.
61. J. Eriksson, "Securitizing IT," in J. Eriksson, ed., *Threat Politics: New Perspectives on Security, Risk and Crisis Management*, Aldershot: Ashgate, 2001; Eriksson,

"Cyberplagues, IT and Security: Threat Politics in the Information Age", *Journal of Contingencies and Crisis Management*, vol. 9, no. 4, 2001, pp. 211-22.

62. Bendrath, 2001, n. 21; Eriksson, ibid.
63. D Saco, "Colonizing Cyberspace: National Security and the Internet", in J. Weldes, M. Laffey, H. Gusterson and R. Duvall, eds., *Cultures of Insecurity: States, Communities and the Production of Danger*, Minneapolis: University of Minnesota Press, 1999.
64. J. Der Derian, "Virtuous War/Virtual Theory," *International Affairs*, vol. 76, no. 4, 2000, pp. 771–88.
65. ibid; J. Everard, *Virtual States: The Internet and the Boundaries of the Nation-State*, London: Routledge, 2000.
66. M. Edelman, *The Symbolic Uses of Politics*, 2nd edn. Urbana: University of Illinois Press, 1964; Edelman, *Political Language: Words that Succeed and Policies that Fail*, New York: Academic Press, 1977; Edelman, *The Symbolic Uses of Politics: With a New Afterword*, Urbana: University of Illinois Press, 1985; Edelman, *Constructing the Political Spectacle*, Chicago, II: Chicago University Press, 1988; R.M. Merelman, ed., *Language, Symbolism, and Politics*, Boulder, CO: Westview Press, 1993; D.O. Sears, "Symbolic Politics: A Socio – Psychological Theory," in S. Iyengar and W.J. McGuire, eds., *Explorations in Political Psychology*, Durham, NC: Duke University Press, 1993.
67. Eriksson and Giacomello, n. 15, p. 235.