ISSN 0973-5011

2020. Vol. 13. No 2

Indian Journal of Politics and International Relations

IJPAIR

Indian Journal of Politics and International Relations

Vol. 13 No.2 (2020)

Editorial Office
School of International Relations and Politics
Mahatma Gandhi University
Priyadarshini Hills P.O.,
Kottayam, Kerala India PIN- 686560 e-mail: vinodan.c@gmail.com

Printed in India at Kottayam, Kerala, India

Indian Journal of Politics and International Relations

Vol. 13 No 2 July- December-2020

ISSN 0973-5011
Indian Journal of Politics and International Relations (2020) **Vol. 13. No 2**

CONTENTS

ISSN 0973-5011
Indian Journal of Politics and International Relations (2020) **Vol. 13. No 2**

THE POLITICS OF INFORMATION WARFARE: SECURITISATION AS RATIONALISATION

Shibu M.P.

Security has its distinctive meaning, which is firmly rooted in the traditions of power politics. What makes something an international security issue can be found in the traditional military-political understanding of security[1]. Security is about survival when a problem is presented as an existential threat to a referent object which needs to be protected. The unique nature of security threat justifies the use of extraordinary measures to handle them. The invocation of security has been the key to legitimising the use of force. It has generally opened the way for the state to mobilise or take extraordinary powers to handle existential threats.

Traditionally, by saying 'security', a state representative declares an emergency condition, claiming a right to use whatever means necessary to block a threatening development. Security is a social problem in the broadest sense since social conditions provide the incentive to use or not to use force. The structure or system of power that states create through their interactions determines how power is used (Kolodziej 2005). As Kenneth Waltz argues, states are concerned about their relative power position within the system of states. It is through this structure of power that states pursue their interests and realise their aims.

Existential threat can be understood only in the context of the particular character of the referent object in question. The existential quality of existence will vary significantly across different sectors and levels of analysis. Therefore, the nature of the existential threat will differ from sector to sector. In the military sector, the referent object is the state, although it may also be other political entities. Information resources have become an essential asset to the state in the era of revolution in information technologies. Hence, protecting vital information resources has become the state's primary objective for survival in a globalised world. International communication has been greatly facilitated and enhanced by new communication technologies, which are being employed as a means by which robust national and international systems radiate out and attempt to extend themselves globally. These expanding economic, political, and cultural systems do not operate in a vacuum; they are protected by powerful military shields and are dependent on information technologies (Mowlana 1990).

In the national security arena, information warfare has become an evolutionary topic of discussion, and the state pursues defensive operations as part of securitisation. Securitisation implies that problems are identified as existential threats that legitimises extraordinary measures such as secrecy or use of violence. At the same time, the state also engages in offensive operations for intelligence purposes. Because of the interplay of both offensive and defensive operations, defensive information operations do not yield the expected result. Nevertheless, technologically powerful countries see securitisation as a case

of rationalisation. In securitisation, framing actors such as politicians, bureaucrats, experts, the media, pressure groups, and academics have an essential role in articulating societal salience. These influential actors or military-industrial-academic-complex as the critical theorist reframed it and maintained a dominant position in framing threats and risks of common interest. Thus security is firmly institutionalised, privileging the government and military through the particular security policies.

Since the mid-1990s, the state has increasingly paid attention to information technologies and dramatised security problems under the title 'Information Warfare'[2]. The revolutionary development of Information Technology (IT) and the emergence of new means of warfare, including hacking, virus attacks, electronic espionage, deception etc. enabled the potentially hostile actors, including the states as well as non-state actors, to take advantage of the vulnerability resulting from the dependency on IT (Eriksson 2001: 214).

Securitisation and Policy Diffusion

Securitisation was extensive because of international policy diffusion, that is an idea or threat image spread from one country to another. Policy diffusion may occur either due to attempts to influence policy in another polity actively or because of imitation. However, ideas continuously change and adapt to agent's demands and circumstances in domestic and international policy networks. Thus, policy diffusion entails a process of communication involving the movement of both ideas and organisational change. In global policymaking, the West significantly dominates other states. For instance, America is the first country to establish a Defence Science Board Task Force for defensive information warfare, which was assigned to identify national interest information users (Fields 1996). It also aims at characterising the procedures, processes and mechanisms required to defend against various classes of threats to the national information infrastructure and the users of national interest information.

Information security and related frames are not something invented in a particular context but inspired and influenced by conceptual and organisational developments in the United States. The notions of 'electronic warfare' and 'information security' had been floating among experts and policymakers for many years. The framing of information warfare came in the early 1990s after the US involvement in the 1990-91 Gulf War against Iraq. It has occurred partly because of general awareness and active monitoring of US security thinking or partly through direct contact and the agents of this policy diffusion, mostly bureaucrats and academics (Haas 1992)**.** For instance, the Swedish government has imitated the US method of testing its own IT security by having the so-called 'Red Teams'[3] making controlled attempts to penetrate information systems. The Swedish government has set up its own 'Red Teams' and imitated a US information warfare exercise called 'Eligible Receiver 97'.[4]

On the other hand, policy diffusion could occur due to the dominant countries' actions or policies. For example, 'the promotion of democracy is central to the George W. Bush Administration's prosecution of both the war on terrorism and its overall grand strategy' (Chomsky 2006: 102)**.** Here, policies, including the dominant state's economic and political ones, must be complied with by the state upon they act. If the state resists this compulsion,

they will be categorised as rogue state[5] or axis of evil, which is then portrayed as a threat to global security. These actions, in a way, impose a kind of state terror upon the adversaries. Chomsky makes a mention of the comment made by historian Arno Mayer:

> America has been the chief perpetrator of pre-emptive state terror and innumerable other rogue actions causing immense harm, always in the name of democracy, liberty and justice (Chomsky 2006: 108).

The final act as part of securitisation is a war against adversaries who do not adhere to fair international laws. Winning in battle needs support, both at home and abroad. Here, the global communication industry plays a role that suits the interests of global powers. Securitisation of the issue helps the attacking country portray the war as a pre-emptive war, which has become a new norm in international relations. It confers the state with the right to attack any state by claiming it to be an imminent threat to global security. The US' Iraq invasion is an example where the US claimed it as a 'pre-emptive war' but was considered a ‘preventive war[7].

Securitisation and Social Problem

Securitisation as a defensive move provides the incentive to use or not to use force when security is considered a social problem. A securitising move does not exist in isolation. It may be subsequently linked to another securitising move that contributes to a securitisation. Securitisation does not reflect how events happened but provides a simplified view of things by concentrating on the outcome rather than the process. If states do not differentiate between existential and ordinary risks in society, security questions can be found everywhere. Hence, security logic implies that particular risks are singled out as existential ones, rather than the equalisation of all risks as it would challenge the security logic itself (Huymans 1998).

The referent objects in society are larger groups that carry the loyalties and devotion of subjects in a form and to the degree that can create a socially powerful argument that this is the threat with which we are threatened. When a threat becomes a national security issue, what type of threat is it and how the recipient state perceives it, and the intensity with which the threat operates are all evaluated. As Barry Buzan argued, the threat's intensity determines the legitimacy for considering it as a national security issue (Buzan 1991).

Threats persist in society when offensive technologies are superior to defensive technologies. Such a situation of offence dominance leads to a security dilemma. Offence-defence theory predicts that security will become more competitive and less peaceful when the offence-defence balance shifts towards the offence. The theory argues that expansionist grand strategies will be more common in a world where there is an offensive advantage and states will adopt offensive military doctrines. Thus, an arms race will emerge, foreign policies will be more aggressive, crises will be frequent and war will become more probable.

In information warfare, security dilemma arises when a technologically superior state prepares for technological innovation in critical information infrastructures. It will create an irresolvable uncertainty in others’ minds regarding whether those preparations are meant for

offensive purpose or not. If the potential enemy believes that the best form of defence is preparing for attack, it may lead to subsequent arms race in offensive military technologies (Butfoy 1997).

Securitisation and Implications for a Democratic State

Advancement in Information Technology determines how power and accountability are structured in a political system, and the interactions between the government and the people. Since there is a correlation between the national security policy and the advancement in technology, it has a more significant impact on political life. In many states like the US, offensive information warfare has become an essential aspect of national security policy. Offensive information warfare, targeting the enemy's information and its functions, is pursued by states while protecting its critical communication infrastructure through defensive information operations. The consequence is less democratic control on the conduct of warfare.

In its offensive form, information warfare raises questions about the democratic control of the new form of military activities whose answers cannot be found in constitutional provisions. Some scholars have argued that if executed correctly, information warfare may very well permit the states to avoid the conventional deployment of troops and munitions. Information warfare changes the rules of warfare, and with the appropriate information, it is possible to accomplish objectives without using force. However, the difference between information warfare and conventional warfare is its method of democratic control. In traditional warfare, defence is treated as more superior than offence (Clausewitz 1982). But in information warfare, such a judgment is impossible due to both offensive and defensive actors' invisibility.

Digital technology and advanced electronic communication determine a country's capabilities in pursuing Revolution in Military Affairs (RMA). Besides, the functioning of large complex intelligence services relies on advanced computer systems. Beyond that, the society in which these institutions are embedded – its industry, financial institutions, transportation, energy distribution etc. depends on how information networks function. Therefore, threats to information networks have both military and civil dimensions.

In Information warfare, there is an asymmetry in vulnerability between states. For instance, the asymmetry between the United States and its adversaries is a case in point. The US' ability to disrupt the information network is more significant than its adversaries because of the former's superiority in information technologies. On the other hand, the United States is more vulnerable to information warfare because of its exceptional dependence on information systems. Thus, in the case of offensive information warfare, the US is dominant and capable of undermining other countries' defences. Far more than any other forms of warfare, profound asymmetries may characterise the cyber war[8]. These vulnerabilities have a profound impact on democratic principles. The free flow of information is a cornerstone of democracy as is the right to privacy, but both may collide with attempts to limit information warfare vulnerabilities.

The spread of information technology within the agencies of the democratic state poses challenges to a variety of values and interests in society. As part of securitisation, the state uses personal information for various administrative, investigative, and analytical purposes. Advancement in technology helps the state to collect and store data, which creates fear that basic human dignity and individuality would be compromised. Nevertheless, technology has become an autonomous social force and an end in itself rather than an instrument to satisfy desires and needs. As Bennett makes a mention of the comment made by Miller:

> Technological improvements in information handling capability have been followed by a tendency to engage in more extensive manipulation and recorded data analysis. This, in turn, has motivated the collection of data pertaining to a large number of variables, which results in more personal information being extracted from individuals (Bennett 1991:63).

Securitisation in Effects-Based Operations

An information operation is one of the tools for a state to influence or coerce other nations, especially in Effects-Based Operations (EBO). The US Air Force definition of EBO is the action taken against an enemy system for the desired military and political outcome. In practice, EBO is the employment of all national power instruments against opposing political, military, economic, social, information and infrastructure capabilities to achieve the desired effect. This is how non-military capabilities are used for securitisation.

Effects-Based Operations expand the range of capabilities available to the political and military decision-makers and dramatically increases the political and military demand for a wide range of information not usually handled by the traditional military. The effort to provide this increased level of information for effect-based operations is called Operational Net Assessment (ONA) [9] by the United States Joint Forces Command (USJFCOM) Joint Futures Lab and was designed to be the data source for EBO planning.

To securitise an issue and apply Effects-Based Operations, information about the crisis is necessary. Without the information, readiness forces will not be able to undertake EBO. Predictive Battle Space Awareness (PBA) [10] is designed to use a wide range of tools to take current information and predict future status. Since information operations benefit from predicting the effect of its actions, likely enemy responses and future enemy activities, Predictive Battle Space Awareness (PBA) supports both Effects-Based Operations (EBO) as well as Information Operations (IO) (Allen 2007).

Concerning technology, offence-defence theory argues that if there is no balance between offensive and defensive military technology, it will result in a security dilemma. Scholars pursuing this theory tried to view the history of warfare and weaponry in terms of interplay between the offence and defence. One of the first attempts to generalise interplay between the offence and defence was Clausewitz's work 'On War'. In his opinion, if both sides are supposedly equal, the defence is more painless than offence. If the reason is superior to the offence, the defence may leave both sides with no incentive to attack.

Wright, in his classic, 'A study of War', argues that the superiority of offence generally results in the following:

> an increase in the probability of war; political expansion, unification and empire building; a decrease in the number of states in the system; shorter duration and lower cost of wars. On the other hand, superiority of defence results in the following: strengthening of local areas thereby facilitating revolts; the disintegration of empires; the decentralisation of states; an increase in the number of states; decrease in the decisiveness of wars and their importance in world politics; strategies of protracted stalemates and mutual attrition that result in the longer duration and greater destructiveness (Wright 1965).

Quester's *Offence and Defence in the International System* argues that offensive superiority is conducive to empire while defensive superiority leads to political independence and prolonged wars. He further argues that a counter-force offensive capability encourages war while a counter-value offensive capability promotes peace (Quester 1977). Jervis has made the most systematic effort to trace the offensive/defensive balances' theoretical impact on the likelihood of war. Using the security dilemma's conceptual device, he identifies that offensive superiority increases the benefits from striking first and increases the cost of allowing the adversary to strike first (Jervis 1978).

If we analyse the offence-defence balance aspect in Information Warfare, offence dominates the defence in today's world. This is mainly due to the technological superiority of certain states in offensive warfare. Here defensive information warfare is a benefit for these technologically superior countries by way of securitisation. By securitising technologies and preventing them from reaching other countries' hands, these states could pursue their offensive information warfare to achieve their desired ends.

Securitisation and the Dimension of Defensive Technologies

Defensive Technologies that are now being deployed by both military and commercial domains provide security layers to bridge the gap between the two approaches. First-generation and expensive military 'trusted' computers are based on formal analysis or testing with strong cryptography. Secondly, commercial technologies – computers, UNIX or Windows Operating Systems and networks – with components like firewalls, software wrappers, smart card authentication etc., help manage risks and achieve a specified degree of security for operation in non-secure GII (Global Information Infrastructure) (Waltz 1998).

Enabling technologies will provide low-cost security to complex heterogeneous networks with open system augmentation that provide layers of protection for secure 'enclaves' and the networks they communicate. These trusted layers – software, hardware walls and barriers – will give security to the entrusted databases, operating systems and other elements under their control. Emerging technologies will increase security and survivability over large-scale networks with autonomous detection, reaction and restoration mechanisms.

Technologies of defensive operations perform functions like encryption, steganography, anonymity, sanitisation, trash disposal and shielding. Cryptography does for electronic information what locks do for printed information. Information is protected by scrambling with a secret key. The scrambled information called 'ciphertext' is unknown to anyone who does not know the key. Producing the ciphertext is called encipherment or encryption and the reverse process of restoring the original message called 'plaintext' is called decipherment or decryption. An encryption system or cypher is built from two basic types of transformations: transpositions and substitutions. Transpositions (permutations) re-arrange bits or characters, whereas substitutions replace bits, characters, or blocks with substitutes. These transformations are keyed so that a single method can be used with different results. Confidentiality encryption is a process of encoding an electronic communication so that only the originator and receiver of the particular message could read it (United Nations 2002). To decrypt, one must know both the method and the key under which it was encrypted. While the key is kept secret, the method itself is often made public to be shared by many people and implemented in hardware and software products[11].

Steganography is the method of hiding a message in such a manner that its very existence is concealed. It is done by embedding the message in some medium such as document, image, sound recording, or video. Anyone who knows the medium containing a secret message could promptly extract the message, assuming that the encoding method is known. The purpose of using steganography is different for different groups in society. The use of steganography by terrorists or non-state actors underlines the concerns that governments feel about the cheap, readily available, powerful encryption tools currently widespread due to the globalisation of information technologies. Civil libertarians see the benefits of strong ciphers as citizens' rights in a free state. They believe that the government's access to the encrypted communications of its citizens could be disastrous if an authoritarian regime comes to power. On the other hand, government agencies fear that criminals such as terrorists, drug runners, and gangsters will use encrypted communications to carry on their activities without interference from the law (Goebel 2007).

Information warfare attacks can be averted by monitoring and controlling access to and use of information resources. Even if an offensive operation is not prevented, monitoring might detect it while it is in progress, allowing the possibility of aborting it before any severe damage is done and enabling timely response. In *War and Anti war*, Alvin Toffler and Heidi Toffler argue that the 'third-wave war' is information warfare. The 'third-wave peace' form is also driven by widespread availability of information to minimise misunderstanding of intentions, actions, and competing parties' goals. Even as information is exploited for intelligence purposes, this information's increasing availability can reduce uncertainty and misunderstanding amongst states. Thus, information technology is a twin-edged sword, offering the potential for cooperation and peace, or its use as an instrument of conflict and war. As with nuclear technology, humankind must be cautious about the applications pertaining to information technology (Waltz 1998).

Offensive information warfare through offensive technologies takes advantage of weaknesses in defensive technologies. States hold military secrets confidentially when the

offence dominates. This causes rational over-arming, as states assess their defence capabilities against the worst-case estimates of enemy strength, based on the notion that underspending is disastrous while overspending is wasteful (Evera 2000). These vulnerabilities can show up in the physical environment, within computers and networks and in human practices. In cyberspace, vulnerability monitoring begins with software installation, as packaged software is often delivered with an initial configuration that leave systems wide open to attack. The operating system used to support a web server might come with default passwords that are trivial for hackers to guess or with the entire file system readable and writable to anyone with access to the system. Security problems can arise anytime when information resources are updated and reconfigured or when new resources are added or old ones are removed. In the United States, federal agencies are mandated by the Office of Management and Budget (OMB)[12] Circular A-130 to conduct security certifications of systems that process sensitive information or perform critical support functions. Certification in this context refers to technical evaluation of compliance of an information system in its operating environment. It is conducted for accreditation, the official authorisation, to put an information system into operational use.

A significant weakness that contributes to the failure of defensive technologies in containing information warfare is the lack of security awareness and training programmes to the operators. Security awareness and training programmes help make employees familiar with the concerned organisation's information security policy; the idea is to securitise them against the risks and potential losses and train them to use security practices and technologies. However, training in these technologies is confined to technologically-dominant countries.

The Information, Computer and Communication Policy (ICCP) Committee of the Organisation for Economic Cooperation and Development (OECD) has formed a group of experts who formulated the information system's security guidelines. The guidelines were approved by the ICCP in October 1992 and adopted by the 24 member countries of the OECD. The guidelines were applied to all information systems in the public and private sectors, which include *accountability*, a*wareness*, *ethics, multidisciplinary*, p*roportionality, integration, timeliness, reassessment, democracy* (Denning 1999).

Despite the formulation and application of several policies, the interplay in terms of offensive and defensive technologies poses a challenge in protecting critical information resources. Encryption policy is one of the most controversial and challenging issues at the turn of the century. Difficulties arise because of two opposing functions: code-making and code-breaking.

Code making refers to the use and development of encryption products that are used for confidentiality protection. It is intended for protecting communications and, to a lesser extent, stored information from adversaries. Encryption is performed by transposing or altering the exact text through an algorithm (a cryptographic function) to a cypher text (Black 2000). Code breaking refers to acquiring access to encrypted data by some means other than the normal decryption process used by the intended recipients of data. Code breaking is achieved either by obtaining the decryption key through a unique key recovery service or

finding the key through cryptography. It helps ensure that information is accessible if decryption keys getting lost, damaged, or destroyed. The code breaking technologies in information warfare are essential in determining military technology's offence-defence balance (Lieber 2000).

Securitisation and Social Construction of Security

In September 2002, US President George W. Bush portrayed Iraq as a grave danger to international security and emphasised the next requirement of a global 'War on Terror' to eliminate the Iraq regime's threat. In subsequent days, Iraq came to be considered as the most dangerous threat to national security**.** There are certain conditions involved in securitising an issue as a grave threat. The Copenhagen School identifies conditions that facilitate the success of security moves. A securitising actor contends that something is in grave danger unless recommended for a particular course of action. A second facilitating condition is that securitising actors have a sufficient degree of social capital or credibility with the audience. Lastly, there are features of alleged threats that can be referred to back up the security claims. The fourth condition is the socialisation of audiences. Therefore, the elements of a securitising move are interpreted through a complex interaction of their content and the viewer's pre-existing perspective. Media also plays an important role as a securitising agent in liberal democracies because of media capital accumulation. Once an issue is accepted as a security issue, political actors can justify the extreme actions for dealing with that issue. It is at this point that a securitising move can be considered successful.

The securitisation and information warfare are related in the case of the Iraq war. The driving force behind the security perception and practice is the language of threat rather than material factors. As compared to the traditional views, securitisation remains mostly unconcerned about the integrity of material evidence. Which means speech creates insecurity. The security claims can be used for political gains, which may be long term or short term. In Iraq's case, short-term gains came essentially in two forms: the electoral gains for Bush and his party and the opportunity to implement their overall political agenda. Second, key members of the Bush administration believed that their long-term goal of re-ordering the Middle East could be achieved if Iraq was securitised (Hughes 2007). The language of threat against Iraq is used efficiently by the Bush administration by quickly pitching the events to his largest audience as a clash of civilisation. The US was portrayed as the victim in yet another good versus evil battle (Huntington 1997).

It was after the Gulf War[13] of 1991 that the securitisation of information infrastructure assumed significance. It was the war where the US and its allies efficiently used offensive information warfare against Iraq. They used satellite imaging systems that can map potential target areas. The maps were put on board Tomahawk cruise missiles during the war and compared with the missile's radar images. The Global Positioning System (GPS), a twenty-four satellite constellation that emits signals used for determining location, helped coalition land forces navigate the desert terrain. It is necessary to securitise these technologies for maintaining their monopoly in warfare. Otherwise, these technologies will quickly be transferred to their adversaries in the globalised era. Even though globalisation provides facilities for the transfer of technologies, the core technologies – whether in nuclear,

information or space – remain in the hands of a few technologically superior countries. Therefore, securitisation could be seen as a more extreme version of politicisation. In principle, the placement of issues on this spectrum is open; depending on circumstances, any problem could end up on any part of the spectrum. As opined by Barry Buzan:

> Politicisation means to make an issue appear to be open, a matter of choice, something that is decided upon and that therefore entails responsibility, in contrast to issues that either could not be different or should not be put under political control (Buzan et al. 1998: 29).

To conclude, securitisation implies presenting an issue as urgent and existential. It is seen as a threat to national security and has to be dealt with authoritatively. This would give legitimisation to offensive operations in information warfare like intelligence operations using information technologies. The securitisation of information technology infrastructures by a technologically superior state affects the international infrastructure because infrastructures are highly interdependent. Thus, securitisation as a defensive operation is pursued by technologically dominated states to maintain their monopoly in the globalised world.

Notes:

The traditional understanding of security refers to a realist construct of security in which the referent object of security is the state. It relied upon in anarchistic balance of power and on the absolute sovereignty of nation-states.

Information warfare has been variously labeled as Cyber war, Network Centric war, Information operation and Command and Control Warfare (C_2 W). Aspin-Brown Commission or Commission on the roles and capabilities of the US Intelligence Community (which submitted its report in 1996) defines information warfare as "activities undertaken by government groups, or individuals to gain electronic access to information systems in other countries… as well as activities undertaken to protect against it".

In the US Army' Red Teaming' is defined as a ‘structured, iterative process executed by trained, educated and practised team members that provides commanders an independent capability to continuously challenge plans, operations, concepts, organisations and capabilities in the context of the operational environment and form partner's and adversaries' perspective’.

Eligible Receiver 97 was the US government's exercise conducted under the No-Notice Interoperability Exercise Programme. The exercise was held during 9-13 June, 1997 which included participants such as National Security Agency (which acted as Red Team), Central Intelligence Agency, Defence Intelligence Agency, Federal Bureau of Investigation, National Reconnaissance office, Defense Information System Agency, Department of State, Department of Justice as well as Critical Civilian Infrastructure providers such as power and communication companies.

Rogue state is the Clinton Administration label to characterise states beyond the international pale that are hostile to the United States. Rogue states were portrayed as being contemptuous of international norms, bent on acquiring weapons of mass destruction and being sponsors of terrorism. Towards the end of the Clinton Administration, the term 'Rogue state' was replaced by the more politically correct term 'States of Concern', which was perhaps an indication of the label's diplomatic disunity. However, the label has been resurrected by the George W. Bush Administration to justify its pursuit of National Missile Defense.

Article 2, Section 4 of the UN Charter speaks about pre-emptive war. It forbids the threat or use of force against any state in the absence of an acute and imminent actual threat. However, Article 51

of the UN Charter permits self-defence. The tension between these two principles is evident in the pre-emptive war doctrine, which claims to be defensive yet does not respond to an attack.

Preventive war aims to forestall a shift in the balance of power by strategically attacking before the balance of power has a chance to shift in the adversary's direction.

Cyberwar, also known as cybernetic war, uses computers and the internet to conduct warfare in cyberspace. It includes web vandalism – attacks that deface web pages, propaganda – spreading political messages to influence public opinion and thereby earning legitimisation of actions, gathering data, attacking critical infrastructures, etc. In its annual report of 2007, the internet security company McAfee reported that approximately 120 countries have been developing ways to use the internet as a weapon and targets are financial markets, government computer systems, and utilities.

Operational Net Assessment (ONA) integrates people, processes, and tools that use multiple information resources and collaborative analysis to build shared knowledge of the adversary and the environment. The ONA concept originated in Rapid Decisive Operations (RDO) war game.

Predictive Battle Space Awareness (PBA) is the state of awareness achieved and maintained by the commander to correctly anticipate future conditions, Intelligence Surveillance and Reconnaissance (ISR) assets which shape the battle space. PBA is a continuous process that provides visualisation, intelligence analysis, exploitation, collaboration, and operational wargaming activities to derive friendly adversary actions.

In certain countries, the application of cryptography for confidentiality purposes is restricted by law for public policy reasons, which involve national defence considerations.

A US Executive Agency established in 1971, with responsibility for preparing and administering the federal budget.

Gulf war is considered infowar, where the US and its allies illustrate information warfare's scope and diversity. Several types of information operations are conducted as part of the Gulf war, including computer intrusions, human spies, spy satellites, eavesdropping, surveillance camera, electronic warfare, physical destruction of communication facilities, perception management, psychological operations etc.

References

Allen, Patrick D. (2007): *Information Operations Planning*, London: Artech House.

Bennett, Colin J. (1991): "Computers, Personal data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s", *Science, Technology and Human Values*, 16(1): 51-69.

Black, J.R. (2000): Message authentication codes, Ph.D. Thesis, University of California.

Butfoy, Andrew (1997): "Offense-Defense Theory and the Security Dilemma: The Problem with Marginalising the Context", *Contemporary Security Policy*, 18(4): 38-58.

Buzan Barry, Ole Waever and Jaap de Wilde (eds.) (1998): *Security: A New Framework for Analysis*, London: Lynne Rienner Publication.

Buzan, Barry (1991): *People States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Colorado: Lynne Reinner Publishers.

Chomsky, Noam (2006): *Failed States: The Abuse of Power and the Assault on Democracy*, New York: Metropolitan books.

Clausewitz, Carl Von (1982): *On War*, Translated by J.J Graham, London: Penguin.

Denning, Dorothy E. (1999): *Information Warfare and Security*, Singapore: Addison Wesely Longman.

Eriksson, Johan (2001): "Cyber plagues, IT, and Security: Threat Politics in the Information Age", *Journal of Contingencies and Crisis Management*, 9(4): 211-222.

Evera, Van Stephen (2000): "Offense, Defense, and the Causes of War" in Michael E. Brown, Owen R. Cote, Sean M. Lynn- Jones and Steven E. Miller (eds.) *Theories of War and Peace*, Cambridge: MIT Press.

Fields, Craig (1996): "Report of the Defense Science Board Task Force on Information Warfare", [Online: web] Accessed on10 May 2008 at URL: http://www.psycom.net/iwar.1.html.

Goebel, Greg (2007): "Frontiers in Cryptography", [Online: web] Accessed on 7 June, 2008 at URL: http://www.vectorsite.net/ttcode_12.html.

Haas, P. M. (1992): "Epistemic Communities and International Policy Coordination", *International Organization*, 46(1): 1-36.

Hughes, Bryn (2007): "Securitizing Iraq: The Bush Administration's Social Construction of Security", *Global Change, Peace and Security*, 19(2): 83-102.

Huntington, Samuel P. (1997): *The Clash of Civilisations and the Remaking of World Order*, New Delhi: Viking.

Huymans, Jef (1998): "Revisiting Copenhagen: Or, on the Creative Development of a Security Studies Agenda in Europe", *European Journal of International Relations*, 4(4): 479-505.

Jervis, R. (1978): "Cooperation under the Security Dilemma", *World Politics*, 30(2):167-214.

Kolodziej, Edward A. (2005): *Security and International Relations*, Cambridge: Cambridge University Press.

Lieber, Keir A. (2000): "Grasping the Technological Peace: The Offense-Defense Balance and International Security", *International Security*, 25(1):71-104.

Mowlana, Hamid (1990): "Communication and International Relations", in Jongsuk Chay (ed.) *Culture and International Relations*, New York: Praeger publishers.

Quester, G. H. (1977): *Offense and Defense in International System*, New York: Wiley Publishers.

United Nations (2002): *UNCTTRAL Model Law on Electronic Signatures with guide to enactment 2001*, United Nations Publications, E.02.V.8, New York.

Waltz, Edward (1998): *Information Warfare Principles and Operations*, London: Artech House.

Wright, Q. (1965): *A Study of War*, Chicago: Chicago University Press.