NATO Library

THEMATIC BIBLIOGRAPHIES
NO.7/2000

'INFORMATION WARFARE'

'LA GUERRE DE L'INFORMATION'

Bibliographies Thématiques
No. 7/2000

Bibliotheque de l'OTAN

WHERE TO CONTACT US :

NATO Library
Office of Information and Press
Room Nb123
1110 Brussels
Belgium

Tel.: (32)2/707.44.14
Fax: (32)2/707.42.49
E-mail: library@hq.nato.int

OU NOUS CONTACTER :

Bibliothèque de l'OTAN
Bureau de l'Information et de la Presse
Bureau Nb123
1110 Bruxelles
Belgique

Tél.: (32)2/707.44.14
Télécopieur: (32)2/707.42.49
Adresse électronique: library@hq.nato.int

HOW TO OBTAIN A PUBLICATION IN THE LIST BELOW :

As a member of the NATO HQ staff you can borrow books (Type: M) for a period of one month and magazines for one week. Reference works (Type: REF) must be consulted in the Library. People from outside NATO can borrow books through their local library via the interlibrary loan system.

COMMENT OBTENIR UNE PUBLICATION MENTIONNÉE DANS LA LISTE CI-DESSOUS :

En tant que membre du personnel de l'OTAN vous pouvez emprunter des livres (Type: M) pour une période d'un mois et des revues pour une semaine. Les livres de référence (Type: REF) sont à consulter sur place. Les personnes n'appartenant pas à l'OTAN peuvent s'adresser à leur bibliothèque locale et emprunter des ouvrages via le système de prêt inter-bibliothèques.

PART I : BOOKS
PREMIERE PARTIE : LIVRES*

Netherlands Annual Review of Military Studies : 1999 : Information Operations - Breda : Royal Netherlands Military Academy, 1999.
ISBN/ISSN:
310 p. : ill.; 24 cm.
ID number: 80016550 Type: M
Library Location: 355.4 /01263
Subject(s):
1. INFORMATION WARFARE
2. INFORMATION OPERATIONS
Added entry(s):
1. Bosch, J. M. J., ed.
2. Luiijf, H. A. M., ed.
3. Mollema, A. R., ed.
4. Royal Netherlands Military Academy (NL)
Bibliography: p. 307-310.

Strategic Appraisal : The Changing Role of Information in Warfare - Santa Monica, CA : Rand Corporation, 1999.
ISBN/ISSN:0833026631
xxiii, 452 p. : ill.; 23 cm.
ID number: 80016392 Type: M
Library Location: 355.4 /01257
Subject(s):
1. INFORMATION TECHNOLOGY--USA
2. INFORMATION WARFARE
Added entry(s):
1. Khalilzad, Zalmay, ed.
2. White, John P., ed.
3. Rand Corporation (US)
'The book is divided into three parts : Part I analyzes the effects of information technology on society and the international system. Part II focuses on the United States and examines what new opportunities and vulnerabilities these new information technologies will present for the United States. Part III focuses on current issues and lessons that today's US decisionmakers need to understand if they are to function in the world to come.'

War in the Information Age : New Challenges for US Security - Washington : Brassey's, 1997.
ISBN/ISSN:1574881183
xxii, 375 p.; 24 cm.
ID number: 80014859 Type: M
Library Location: 355.4 /01217
Subject(s):
1. MILITARY ART AND SCIENCE
2. INFORMATION TECHNOLOGY
3. INFORMATION WARFARE
Added entry(s):
1. Pfaltzgraff, Robert L., ed.
2. Schultz, Richard H., ed.
Includes index.
'This book takes a close look at the future face of battle. The contributors address the security implications of an increasing reliance on information technologies for competitiveness, economic infrastructure, and military operations. Topics include the emerging information-age security environment; assembly, analysis, and

* This list contains material received as of September 2000 – Cette liste est arrêtée au 19 septembre 2000.

distribution of war information; and operational issues of maneuver, precision-strike and joint/combined operations. This work represents the first serious effort to examine how the information age is shaping security environments and the conduct of warfare as we move into the twenty-first century.'

Freedman, Lawrence
The Revolution in Strategic Affairs - Oxford, UK : Oxford University Press, 1998.
ISBN/ISSN:0199223696
87 p.; 24 cm.
(Adelphi papers, 0567-932X ; 318)
ID number: 80014815 Type: M
Library Location: 623 /00832
Subject(s):
1. RMA
2. INFORMATION WARFARE
3. STRATEGY
Added entry(s):
1. International Institute for Strategic Studies (GB)
'Rapid developments in information technology and precision weaponry have led many analysts and practitioners to herald a 'revolution in military affairs' (RMA), making possible quick and decisive victories with minimal casualties and collateral damage. This paper argues that important changes are under way which may indeed be revolutionary in their impact. However, the issues that drive conflict will persist, and many of the technical advances associated with the RMA will not necessarily produce a transformation in the nature of warfare. The end of the Cold War has meant that another revolution - one in political affairs - has taken place. In this new political setting, major powers appear less likely to go to war with one another than they are to intervene in conflicts involving weak states, militia groups, drug cartels and terrorists. The precision-guided weapons and space-based infrastructure at the heart of the RMA may be less suited to conflicts such as these. If the cumulative effect of the changes outlined above is to produce a revolution, it is a revolution in strategic, as much as military, affairs.'

Schmitt, Michael N.
Computer Network Attack and the Use of Force in International Law : Thoughts on Normative Framework - [s.l.] : US Air Force Academy, 1999.
ISBN/ISSN:
viii, 61 p.; 23 cm.
(Research Publication ; 1)
ID number: 80016139 Type: M
Library Location: 341.3 /00101
Subject(s):
1. INFORMATION OPERATIONS
2. WAR (INTERNATIONAL LAW)
3. USE OF FORCE (INTERNATIONAL LAW)
Added entry(s):
1. US Air Force Academy. Institute for Information Technology Applications
'This book explores the acceptability under the jus ad bellum, that body of international law governing the resort to force as an instrument of national policy, of computer network attack. Analysis centers on the United Nations Charter's prohibition of the use of force in Article 2(4), its Chapter VII security scheme, and the inherent right to self-defense codified in Article 51. Concluding that traditional applications of the use of force prohibition fail to adequately safeguard shared community values threatened by CNA, the Article proposes on alternative normative framework based on scrutiny of the consequences cuased by such operations.'

Virilio, Paul
Strategie de la deception - Paris : Galilee, 1999.
ISBN/ISSN:2718605243
87 p.; 22 cm.
(L'espace critique)
ID number: 80016326 Type: M
Library Location: 355.4 /01253
Subject(s):
1. NATO--ARMED FORCES--KOSOVO (SERBIA)
2. INFORMATION WARFARE
3. STRATEGY
'Dans les Balkans, l'OTAN a fait une experience a ses depends : on ne bombarde pas une guerre civile. Demi-guerre non declaree, demi-defaite ou demi-victoire annoncee, la fin du conflit du Kosovo ne resoud aucun des problemes politiques de l'Europe. Victime pendant 40 annees d'une strategie de la dissuasion, fondee sur le primat de l'arme de destruction massive, notre continent voit maintenant lui succeder cette strategie de la deception qui repose sur les capacites cybernetiques de l'information massive, mais surtout sur celles d'une desinformation generalisee. Sous le vocable de la 'global information dominance', les Etats-Unis, ultime grande puissance, lancent maintenant la 'revolution des affaires militaires'. Face a l'inevitable proliferation des armes de destruction massive, mais aussi bien des actes de terrorisme, a l'arret du flux des ressources vitales, au mouvement incontrole et massif des populations, le nouveau concept strategique elabore a Washington a l'occasion du cinquantieme anniversaire de l'OTAN, s'engage dans la voie du controle et de la surveillance tous azimuts des phenomenes paniques que ne manquera pas de provoquer demain la mondialisation.'

Wautelet, Michel
Les cyberconflits : Internet, autoroutes de l'information et cyberspace : quelles menaces ? - Bruxelles : GRIP, 1998.
ISBN/ISSN:2870277113
102 p. : ill.; 21 cm.
(Publications du GRIP ; 228)
ID number: 80014781 Type: M
Library Location: 623 /00830
Subject(s):
1. INFORMATION WARFARE
2. COMPUTER NETWORKS
3. INFORMATION HIGHWAYS
4. INTERNET (COMPUTER NETWORK)
Added entry(s):
1. Institut Europeen de Recherche et d'Information sur la Paix et la Securite (BE)
'Piratage des ordinateurs du Parlement europeen, introduction de messages antisemites dans le site repute protege du FBI, infiltration de celui du Pentagone, 'bombardement electronique' d'un institut de communication en Espagne ... Malgre son histoire encore recente, le reseau Internet a deja connu quelques deboires. Au-dela de ces incidents, que presage l'avenir ? Internet n'etant que le precurseur des autoroutes de l'information et du cyberspace, serons-nous demain sous la menace de conflits d'un genre nouveau, ou le soldat aura cede le pas au pirate informatique, ou les guerres se deplaceront du terrain militaire vers celui du civil ? Le risque est reel et doit etre pris au serieux. Car en paralysant le transport aerien, en rendant inoperant le reseau electrique, en faussant le systeme bancaire ... via le cyberspace, il serait possible de destabiliser une entreprise, voire l'economie de tout un pays ! Presenter de maniere attrayante et accessible ce nouveau concept de 'cyberconflit', tel est l'objet du present ouvrage. Apres avoir examine le cyberspace lui-meme et ses differents composants (elements materiels, logiciels et humains), l'auteur se penche sur ces 'cyberconflits' : leurs caracteristiques, les divers acteurs, les cibles principales ... Et de conclure sur une interrogation : le cyberspace, ne pourrait-il aussi jouer un role positif sur le plan de la securite internationale, en

tant qu'outil de prevention des conflits ?'

PART II : MAGAZINE ARTICLES
*DEUXIEME PARTIE : ARTICLES DE REVUES***

- Guerre de l' information et intelligence economique et strategique.
  ARMEMENT, no. 60, decembre 1997 - janvier 1998, numero entier.

- Arquilla, John
  Karmel, Solomon M.
  Welcome to the Revolution...in Chinese Military Affairs.
  DEFENSE ANALYSIS, vol. 13, no. 3, December 1997, p. 255-269.

  In this paper the authors explore Chinese thinking in the areas of "information warfare" and the "Revolution in Military Affairs", as most of the ferment in military thought currently revolves around the changes in warfare likely to be wrought by recent and newly emerging advances in information technologies. After advancing some working definitions of these concept, and developing a few of their key implications for the future of conflict, drawn from Western views, they survey the Chinese literature to search out the various similarities and differences in emerging strategic thought. Finally, they consider what the West may learn from the Chinese approach, and theorise about China's prospects for achieving revolutionary change-and the effects this might have upon the international system.

- Ayers, Robert
  The New Threat : Information Warfare.
  RUSI JOURNAL, vol. 144, no. 5, October 1999, p. 23-27.

- Barnett, Roger W.
  Information Operations, Deterrence, and the Use of Force.
  NAVAL WAR COLLEGE REVIEW, vol. 51, no. 2, Sequence 362, Spring 1998, p. 7-19.

  For the US military, the topics of central interest in information operations narrow down to two : deterrence and employment. Deterrence of an information attack against the United States and its friends and allies, and the use of information operations in the affairs of state constitute the dual focus of attention. This article examines deterrence as it relates to information operations and then offers some insights on employment. It argues first that for the two types of deterrence - general and immediate (or 'focused') - the United States has inherent strengths but also identifiable shortcomings that can be rectified. Second, this article contends that there are important and valid arguments against allowing information operations to be characterized as 'uses of force' in international law. The more routinely 'information operations' can be understood, like 'counter-terrorism', as self-defense not involving 'the use of force', the greater will be its contribution to US national security.

** This list contains material received as of September 2000 – Cette liste est arrêtée au 19 septembre 2000.

- Bosch, J. M. J.
  Information Operations - Challenge or Frustration ?
  MILITARY TECHNOLOGY, vol. 24, no. 5, 2000, p. 86-89.

  Information Operations can only be understood in the broader context of change and continuity. Cyberspace is, like land, sea, air and space a dimension in which war can be waged, where defence is a necessity while attack is a possibility. There is a close relationship between information-based warfare and Information Operations; IOs do not only impact the military domain, they may also influence national, international and even global layers of connectivity. In the end all layers need command and control to keep order in the system. After all it is man who decides and acts. We face new threats; the challenge is here and now. The frustration comes with the complexity of the challenge.

- Centner, Christopher M.
  Precision-Guided Propaganda : Exploiting the US Information Advantage in Peacetime.
  STRATEGIC REVIEW, vol. 25, no. 2, Spring 1997, p. 35-41.

  This article describes the growing potential of propaganda to support peacetime policy in the modern information age. It describes how propaganda is affected by technology, and how new information technology presents propagandists with an opportunity to effectively target single points - specific individuals and influential segments. This article focuses solely upon propaganda efforts directed outward, to foreign nations and organizations, and not to propaganda directed inward toward US citizens.

- Cilluffo, Frank J.
  Gergely, Curt H.
  Information Warfare and Strategic Terrorism.
  TERRORISM AND POLITICAL VIOLENCE, vol. 9, no. 1, Spring 1997, p. 84-94.

  This article examines the changing nature of terrorism, discusses the attributes of IW and the potential impact and consequences of an IW attack, examines the vulnerability of the United States to an IW attack, and describes the risks of such attacks. In the final portion of the article, the authors present recommendations for dealing with the use of IW tactics by terrorists.

- Cimbala, Stephen J.
  Accidental/Inadvertent Nuclear War and Information Warfare.
  ARMED FORCES AND SOCIETY, vol. 25, no. 4, Summer 1999, p. 653-675.

  Because of military professional enthusiasm for a post-nuclear world dominated by high technology, conventional weapons may be misplaced. Nuclear deterrence remains highly relevant to the new world order because of residual great power nuclear arsenals and nuclear proliferation. In addition, the possible combination of information warfare and a failure of nuclear deterrence is one troublesome aspect of the future technology and policy environment. Stable nuclear deterrence depends upon an environment of mutual confidence and accurate information exchange between potential adversaries, especially during crises. Information warfare is intended to corrupt the information environment of potential opponents before a war begins or during it. Infowarriors could increase the likelihood of accidental/inadvertent nuclear war or escalation.

- Cimbala, Stephen J.
  Information Warfare and Nuclear Conflict Termination.
  EUROPEAN SECURITY, vol. 7, no. 4, Winter 1998, p. 69-90.

  This study considers the possible implications of information warfare for efforts to terminate a nuclear war, or a war between nuclear armed states that is about to go nuclear. Information warfare could interfere with some of the requirements for nuclear conflict termination in at least five ways : by increasing the difficulty of accurate communication between heads of state; by decreasing the likelihood of military compliance with terms of ceasefire or settlement; by reinforcing mass images of the enemy that make it more difficult for leaders to negotiate; and by making battle damage assessment more complicated; and by increasing the amount of uncertainty within an already chaotic government decision-making process and within a possibly acephalous military instrument.

- Cimbala, Stephen J.
  Nuclear Crisis Management and Information Warfare.
  PARAMETERS, vol. 29, no. 2, Summer 1999, p. 117-128.

  First, the author explains why the issue of nuclear deterrence remains significant after the Cold War. Second, he discusses what governments must do in order to perform successfully the crisis management function and the complexity inherent in accomplishing these tasks. Third, he identifies some of the ways in which information warfare may increase the difficulty of accomplishing those tasks necessary to reduce or eliminate the risks of failed crisis management, with attention to the special character of crises between nuclear-armed states. Fourth, he acknowledges that information warfare cannot be done away with, and is in some cases a desirable option for US policymakers. Therefore, the lion of infowar must be made compatible with the lamb of nuclear deterrence (or is it the reverse ?).

- Critchlow, Robert D.
  Whom the Gods Would Destroy : An Information Warfare Alternative for Deterrence and Compellence.
  NAVAL WAR COLLEGE REVIEW, vol. 53, no. 3, Sequence 371, Summer 2000, p. 21-38.

  The ability of the US nuclear arsenal to deter and compel smaller WMD-owning adversaries is growing smaller; an alternative strategy is required. Information warfare can provide that alternative.

- Dean, Sydney E.
  Information Warfare : Entscheidet zukunftig die Information ?
  EUROPAISCHE SICHERHEIT, 48. Jg., Nr. 11, November 1999, S. 24-26.

  Modern societies are to large extent dependent on information and communication. The centerpieces of today's information society are computers and computerized systems which exchange data by cable or radio (wireless). Almost the entire spectrum of the modern civilian and military infrastructure depends on the interlinkage with other systems and on the exchange of information via digital networks. This does not only apply to industrial states, but also to states with a medium level development and to an astonishing degree also to many developing countries. A long-term study of the American Air University - Air Force 2025 - asserts that in future 'influence will be exerted more by information than by bombs'.

- Devost, Matthew G.
  Houghton, Brian K.
  Pollard, Neal Allen
  Information Terrorism : Political Violence in the Information Age.
  TERRORISM AND POLITICAL VIOLENCE, vol. 9, no. 1, Spring 1997, p. 72-83.

  Information warfare represents a threat to American national security and defense. There are two general methods in which a terrorist might employ an information terrorist attack : (1) when information technology (IT) is a target, and/or (2) when IT is the tool of a larger operation. The first method would target an information system for sabotage, either electronic or physical, thus destroying or disrupting the information system itself and any information infrastructure (e.g. power, communications, etc.) dependent upon it. The second would manipulate and exploit an information system, altering or stealing data, or forcing the system to perform a function for which it was not meant (such as spoofing air traffic control). A perennial dilemma of combating terrorism in a democratic society is finding the right balance between civil liberties and civil security. The special problems associated with IT are examined. The US national security establishment needs to use a flexible, integrated response to counter information terrorists - one which employs information warfare tactics tailored to counter gray-area phenomena, but which also pools resources from 'conventional' counter-terrorism and law enforcement authorities.

- Emmett, Peter
  Information Mania : A New Manifestation of Gulf War Syndrome ?
  RUSI JOURNAL, vol. 141, no. 1, February 1996, p. 19-26.

  The author here traces the origins of Information Warfare, its growth to prominence in military thinking and the dangers inherent in total reliance on it. Information Warfare is a key component of military doctrine when planning for the battlefield of the future. It is the only factor of importance in meeting military requirements into the 21st century.

- Faucon, Felix
  Guerre de l' information ou operations d' information ?
  DEFENSE NATIONALE, 54eme annee, no. 3, mars 1998, p. 65-77.

- Feaver, Peter D.
  Blowback : Information Warfare and the Dynamics of Coercion.
  SECURITY STUDIES, vol. 7, no. 4, Summer 1998, p. 88-120.

- Grove, Gregory D.
  Goodman, Seymour E.
  Lukasik, Stephen J.
  Cyber-attacks and International Law.
  SURVIVAL, vol. 42, no. 3, Autumn 2000, p. 89-103.

  Governments and critical infrastructures rely increasingly on network computing technologies and are thus ever more vulnerable to cyber-attacks. Responding to such attacks - whether through diplomatic or economic sanctions, cyber-counterattack, or physical force - raises legal questions. International customary law is not yet fully formed on this issue, but the UN Charter and the laws of armed conflict establish certain baseline rules. Countries with a stake in evolving legal standards for the use of force in information operations should be prepared to make hard choices. Such countries should aim not only to preserve their own security, but also to set legal precedents that balance the need to use a new kind of force against the considerable, untested risks of doing so.

- Harknett, Richard J.
  Information Warfare and Deterrence.
  PARAMETERS, vol. 26, no. 3, Autumn 1996, p. 93-107.

  Information warfare is best understood by focusing on the concept of connectivity as both a societal and military asset. For strategists seeking to deter this new form of war, connectivity is a double-edged sword. Deterrence requires that the capability to inflict retaliatory costs be perceived as reliable. Deterrence weakens to the degree that the deterrent capability can be contested by a challenger through degradation or avoidance. The inherent accessibility of information technology invites challenges to a network's connectivity. Deterrent threats relying on such connectivity will be susceptible to technical, tactical and operational contest. The contestability of connectivity will make deterrence of information warfare difficult. This article concludes that deterrence models developed during the Cold War will provide poor guidance for strategic thinking about this new form of war, which is better understood in the context of offense and defense.

- Harley, Jeffrey A.
  Information, Technology, and the Center of Gravity.
  NAVAL WAR COLLEGE REVIEW, vol. 50, no. 1, Sequence 357, Winter 1997, p. 66-87.

  What can the United States do to fight better ? The answer is twofold. First, the limitations of information and technology as tools of war need to be recognized and their risks assessed. Secondly, planning must acknowledge that overwhelming force may not always be possible. In that connection, the utility of the center of gravity for planning warrants exploration.

- Henry, Ryan
  Peartree, C. Edward
  Military Theory and Information Warfare.
  PARAMETERS, vol. 28, no. 3, Autumn 1998, p. 121-135.

  This article reviews the effects of information technologies on military theory, tempered by insights into the consequences of previous technological revolutions. Issues emerge that are independent of any technology or international security environment. They include an appraisal of the ability of contemporary analysts and theorists to challenge promises of unprecedented change, and an examination of the theoretical implications of the so-called 'revolution in military affairs'. Related issues include the need to avoid being dazzled by the new technologies (while not exaggerating their significance) and at the same time appreciating the extraordinary near-term advantages and capabilities they afford. Finally there is the matter of balance. We must use the technologies to advantage, neither misapplying them in haste nor hesitating until we miss the opportunities they represent.

- Jacobson, Mark R.
  War in the Information Age : International Law, Self-Defense and the Problem of 'Non-Armed' Attacks.
  JOURNAL OF STRATEGIC STUDIES, vol. 21, no. 3, September 1998, p. 1-23.

  The end of the Cold War and the unprecedented pace of technological change have resulted in a plethora of non-traditional threats to US national security. Indeed, the United States now faces some 'non-traditional' military threats that may exploit its vulnerabilities as a nation whose domestic strength is founded on an information based economy. While international law supports the rights of the United States to act, within limits, in self-defense against deliberate, aggressive, hostile attacks; some would argue that 'non-armed' assaults, such as some forms of information warfare, may not manifest themselves in such a way for a nation to claim the right of self-defense. The work argues that international law and custom, suggest that the United States has the

right to take action, even military action to defend itself against 'non-armed' attacks and that attacks against the US National Information Infrastructure would require such a response. Specifically, the article addresses the question : under what conditions would pre-emptive action be justified when non-armed, yet deliberate, aggressive and hostile action is taken against the United States.

- Kopeinig, Arnulf
  Information Warfare : Versuch eines definitorischen Zugangs im Rhamen politikwissenschaftlicher Untersuchungen.
  OESTERREICHISCHE MILITAERISCHE ZEITSCHRIFT, 37. Jg., Heft 1, Janner - Februar 1999, S. 23-36.

- Lavault, Patrice
  Contre-renseignement, contre-ingerence et maitrise de l' information.
  DEFENSE NATIONALE, 54eme annee, no. 11, novembre 1998, p. 56-67.

- Martin, Daniel
  Cyber-terrorisme : le nouveau peril.
  POLITIQUE INTERNATIONALE, no. 77, automne 1997, p. 299-312.

  It has become axiomatic that in the new information age, knowledge is power. But although the world's economic, financial and military sectors are now totally dependent on computers, the information systems of major corporations and state administrations are highly vulnerable to attacks from individuals, terrorist groups and rogue states. Information technology (IT) terrorism is a new type of threat; it is also a particularly formidable one, since it requires few resources and its potential victims have yet to wake up to the reality of the situation. This has ushered in an increasingly dirty 'info-war', where the objective is to gain access to competing company or state files, either to make use of them or to destroy them. If we wish to preserve the security and stability of developed countries, it is vital that we develop both an effective IT deterrent and an economic intelligence policy embracing industrial groups, financial institutions and public authorities.

- Minkwitz, Olivier
  Schofbanker, Georg
  Information Warfare : die Rustungskontrolle steht vor neuen Herausforderungen.
  OESTERREICHISCHE MILITAERISCHE ZEITSCHRIFT, 38. Jg., Heft 5, September - Oktober 2000, S. 587-594.

- Molander, Roger C.
  Riddile, Andrew S.
  Wilson, Peter A.
  Strategic Information Warfare : A New Face of War.
  PARAMETERS, vol. 26, no. 3, Autumn 1996, p. 81-92.

- Nerlich, Uwe
  Strategische Dimensionen der Informationskriegfuhrung.
  EUROPAISCHE SICHERHEIT, 47. Jg., Nr. 4, April 1998, S. 40-43.

- Peters, Ralph
  Constant Conflict.
  PARAMETERS, vol. 27, no. 2, Summer 1997, p. 4-14.

  The author examines here the global expansion of information and its potentially destructive effects on individuals and cultures unable to master the new technologies on which it rests. He predicts that the next century will see 'constant conflict' in a variety of forms, due largely to the differences between cultures that can master the new technologies and those that cannot. As a consequence, he observes, 'at any given moment for the rest of our lifetimes, there will be multiple conflicts in mutating forms around the globe.'

- Rathmell, Andrew
  Cyber-Terrorism : The Shape of Future Conflict.
  RUSI JOURNAL, vol. 142, no. 5, October 1997, p. 40-45.

  Not only has the socio- and geo-political climate changed dramatically in the last decade, but there has also been a technological sea-change with the advent of the 'information revolution'. The potential that these developments have created for differing forms of 'warfare' in cyberspace seems unlimited, with 'cyber-terrorism' an apparently logical outcome. But this potential needs to be approached not in the spirit of futurology and science-fiction, but with clear-headed analysis. Here the author brings to bear such an approach in discussing Information Warfare and its potential use by sub-state groups, looking at the extent of IW techniques, who would use them, how and what categories of activities they would be involved in. Using the case study of the Provisional IRA as a 'doomsday scenario', he assesses the threat of strategic infrastructure warfare. Dr. Rathmell concludes that as with the rest of society, sub-state groups have embraced the information revolution, but realizing its full potential would require levels of financial and personnel investment unlikely to be achieved soon. What is needed now is a full, pro-active review of vulnerabilities across the information spectrum to ensure we are fully equipped to meet and outflank this new threat when its does materialise.

- Rathmell, Andrew
  Mind Warriors at the Ready.
  WORLD TODAY, vol. 54, no. 11, November 1998, p. 289-291.

  In August, Iraq ended cooperation with UN weapons inspectors looking for weapons of mass destruction. The senior US inspector, Scott Ritter subsequently resigned amidst accusations of a lack of support for the task from the UN and Washington. Strategies for dealing with Saddam Hussein are once again in the spotlight. Could techniques like information warfare and psychological operations offer success where conventional warfare has not ?

- Schwartau, Winn
  Asymmetrical Adversaries.
  ORBIS, vol. 44, no. 2, Spring 2000, p. 197-205.

- Theuerkauf, Thomas
  Informations-Operationen.
  EUROPAISCHE SICHERHEIT, 49. Jg., Nr. 2, Februar 2000, S. 14-18.

  Already today is the information and communications technology both in the civilian and military fields the dominating influence factor for the effectiveness of an overall system. Information requirements in the armed forces increase constantly, among other things due to the wide variety of thinkable missions, the higher dynamics of military operations and the growing efficiency of reconnaissance, command control and weapon systems as well as the application of the information and communications technology. Information operations must be regarded as a new form of

fighting out conflicts between nations or other organizations, groupings and individual actors.

- Thomas, Timothy L.
  Deterring Information Warfare : A New Strategic Challenge.
  PARAMETERS, vol. 26, no. 4, Winter 1996 - 1997, p. 81-91.

  This article explores the idea of deterring information-based assaults. It defines the concept of an information assault and describes and explores the need of forms of deterrence tailored specifically to the threat posed by the use of electronic means as weapons.

- Thomas, Timothy L.
  Dialectical versus Empirical Thinking : Ten Key Elements of the Russian Understanding of Information Operations.
  JOURNAL OF SLAVIC MILITARY STUDIES, vol. 11, no. 1, March 1998, p. 40-62.

- Thomas, Timothy L.
  Kosovo and the Current Myth of Information Superiority.
  PARAMETERS, vol. 30, no. 1, Spring 2000, p. 13-29.

  This article looks at the conflict between NATO and Yugoslavia not from the standpoint of the intent or success of the air campaign (although these issues will be touched upon) but rather through the prism of information superiority. Information superiority allowed NATO to know almost everything about the battlefield, but NATO analysts didn't always understand everything they thought they knew.

- Thomas, Timothy L.
  The Mind Has No Firewall.
  PARAMETERS, vol. 28, no. 1, Spring 1998, p. 84-92.

  This article examines energy-based weapons, psychotronic weapons, and other developments designed to alter the ability of the human body to process stimuli. One consequence of this assessment is that the way we commonly use the term 'information warfare' falls short when the individual soldier, not his equipment, becomes the target of attack.

- Thomas, Timothy L.
  Russia's Information Warfare Structure : Understanding the Roles of the Security Council, FAPSI, the State Technical Commission and the Military.
  EUROPEAN SECURITY, vol. 7, no. 1, Spring 1998, p. 156-172.

  During the past two years, Russia has made significant progress in improving its infrastructure responsible for information security. Security specialists also have produced a draft information security doctrine (which the US does not possess) that discusses critical information issues and areas, and the internal and external information threats to the state. The primary organizations responsible for information security in Russia are the Security Council, responsible for national interests affected by the information age; the Federal Agency for Government Communications and Information (FAPSI), responsible for ensuring the security of state communications and conducting intercept operations; the State Technical commission, devoted to the development of international laws, licensing and certification of IW related policies; and the Russian armed forces, responsible for studying the impact of information operations on military art.

- Tomes, Robert R.
  Boon or Threat ? : The Information Revolution and US National Security. NAVAL WAR COLLEGE REVIEW, vol. 53, no. 3, Sequence 371, Summer 2000, p. 39-59.

  The 'information revolution' has come to dominate national security planning as much as it has come to dominate economic and social life. But this revolution, building on and subsuming previous post-World War II 'revolutions', represents more than cumulative technological advances.

PART III : ELECTRONIC SOURCES
TROISIEME PARTIE : SOURCES ELECTRONIQUES

You will find here a choice of references downloaded from various electronic sources. Some of the articles mentioned are held in print in the Library, others are subscribed to electronically, some are only available through interlibrary loan. So please bear in mind that a certain delay might occur when requesting copies of the articles hereunder.

Vous trouverez ci-dessous un choix de références déchargées de différentes sources électroniques. Certains des articles mentionnés sont conservés par la Bibliothèque en version papier, d'autres peuvent être consultés électroniquement. Quelques-uns, enfin, ne sont disponibles que via le prêt inter-bibliothèques. Veuillez donc noter qu'un certain délai est parfois nécessaire avant d'obtenir une copie des articles cités ci-dessous.

AIR UNIVERSITY LIBRARY INDEX TO MILITARY PERIODICALS

1 Information operations--coming of age?. Andrew Rathmell. Jane's Intelligence Review. vol 12 no 5 (May 2000) :pp 52-55.
2 Information operations--coming of age?. Andrew Rathmell. Jane's Intelligence Review. vol 12 no 5 (May 2000) :pp 52-55.
3 Don't techno for an answer: The false promise of information warfare. Brent Stuart Goodwin. Naval War College Review. vol 53 no 2 (Spring 2000) :pp 215-224.
4 Russian lessons learned from the battles for Grozny. Timothy L. Thomas, LtCol, Ret, Lester W. Grau, LtCol, Ret. Marine Corps Gazette. vol 84 no 4 (Apr 2000) :pp 45-48.
5 Extending network-centric warfare to coalition crisis management and assessment. Dennis M. Gormley, Douglas M. Hart. RUSI. vol 145 no 2 (Apr 2000) :pp 67-72.
6 C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance). Julien Mathonniere. Jane's Defence Weekly. vol 33 no 17 (Apr 26 2000) :pp 36-38.
7 Cyber warfare: Protecting military systems. Lionel D. Alford, Jr, LtCol. Acquisition Review Quarterly. vol 7 no 2 (Spring 2000) :pp 100-120.
8 Kosovo and the current myth of information superiority. Timothy L. Thomas, LtCol, Ret. Parameters. vol 30 no 1 (Spring 2000) :pp 13-29.
9 Information systems sculpt Army's engagement goals. Henry S. Kenyon. Signal. vol 54 no 8 (Apr 2000) :pp 33-35.
10 Information systems sculpt Army's engagement goals. Henry S. Kenyon. Signal. vol 54 no 8 (Apr 2000) :pp 33-35.
11 Cyberspace invaders: Air Force takes the offensive on electronic battlefield. Bryant Jordan. Air Force Times. vol 60 no 33 (Mar 13 2000) :pp 24.
12 Briefing: Russia's Chechen war--second time lucky?. Michael Orr. Jane's Defence Weekly. vol 33 no 10 (Mar 8 2000) :pp 32-36.
13 A vision for PSYOP (psychological operations) in the information age. Paul R.M. Brooks, Jr, Maj. *Special Warfare*. vol 13 no 1 (Winter 2000) :pp 20-24.
14 A new form of warfare. James J. Schneider. Military Review. vol 80 no 1 (Jan-Feb 2000) :pp 56-61.
15 An alternative to the `system of systems'. F.G. Hoffman, LtCol. Marine Corps Gazette. vol 84 no 1 (Jan 2000) :pp 18-22.
16 Network centric warfare: Developing and leveraging information superiority. David S. Alberts, and others. U.S. Naval Institute Proceedings. vol 125 no 12 (Dec 1999) :pp 78+.
17 Cyberterrorism hype. Jane's Intelligence Review. vol 11 no 12 (Dec 1999) :pp 48-52.
18 Information warfare in Kosovo. Zachary P. Hubbard, LtCol. Journal of Electronic Defense. vol 22 no 11 (Nov 1999) :pp 57-58+.
19 Navy to establish `Network Centric' center. Robert Holzer. Navy Times. vol 49 no 7 (Nov 22 1999) :pp 21.

20 Computer break-ins emphasize weakness: Pakistani hackers infiltrate Defense Department Web sites. William Matthews. Air Force Times. vol 60 no 15 (Nov 15 1999) :pp 28.
21 The new threat: Information warfare. Robert Ayers. RUSI. vol 144 no 5 (Oct 1999) :pp 23-27.
22 Pentagon task forces will assist civilian authorities. William Matthews. Air Force Times. vol 60 no 12 (Oct 25 1999) :pp 18.
23 Working together to make the modernization vision a reality. Paul J. Hoeper. Army. vol 49 no 10 (Oct 1999) :pp 39-40+.
24 A problem--and an opportunity for the AOC (Association of Old Crows). Paul G. Kaminski. Journal of Electronic Defense. vol 22 no 9 (Sep 1999) :pp 55-56.
25 Situational awareness: Turning data into knowledge. Sean Carroll. Journal of Electronic Defense. vol 22 no 9 (Sep 1999) :pp 51-52+.

MASTERFILE PREMIER

Record: 1
Title: Opportunity Lost.
Subject(s): DISCLOSURE of information; WAR—Yugoslavia—Serbia; INFORMATION warfare; AIR warfare
Source: Aerospace Power Journal, Summer2000, Vol. 14 Issue 2, p56, 23p, 3bw
Author(s): Pounder, Gary
Abstract: Provides information on a study which examined the control and release of military information to the public during the air war against Serbia. Revolution of information operations; Public information and the new media environment; Reason for the failures in the public-information campaign in Serbia.
AN: 3258216
ISSN: 0897-0823

Record: 2
Title: Internet Leverages the Battlefield.
Subject(s): UNITED States.—Joint Economic Committee; INFORMATION warfare Source: Security Management, Jun2000, Vol. 44 Issue 6, p36, 2p Author(s): Neeley, Dequendre
Abstract: Focuses on the testimony of witnesses before a United States (U.S.) Joint Economic Committee hearing about the appearance of doctrine and dedicated offensive cyber warfare programs in other countries. Remarks from John Serbian Jr., a U.S. Central Intelligence Agency information operations issue manager.
AN: 3325247
ISSN: 0145-9406

Record: 4
Title: A glimpse of cyberwarfare.
Subject(s): COMPUTER crimes; INFORMATION warfare; ESPIONAGE—Technological innovations; INTERNET fraud
Source: U.S. News & World Report, 03/13/2000, Vol. 128 Issue 10, p32,2p, 2c
Author(s): Strobel, Warren P.
Abstract: Focuses on governments who use the Internet in attacks against political adversaries. Details of information-warfare capabilities under development in a number of nations, including Russia, China, and Iraq; Electronic espionage committed against the United States; The difficulty of regulating Internet attacks. INSET: Suspect software, by David E. Kaplan.
AN: 2855041
ISSN: 0041-5537

Record: 6
Title: Electronic Warfare: Battles Without Bloodshed. Subject(s): INFORMATION warfare—United States; ELECTRONICS in military engineering Source: Futurist, Jan/Feb2000, Vol. 34 Issue 1, p23, 4p, 3c Author(s): Stauffer, Don Abstract: Discusses the use of electronic warfare by the United States in support of conventional war goals. How electronic warfare developed; Importance of air power in World War II; Fears on the use of electronic warfare; Development of countermeasures against electronic warfare. INSET: Y2K Drills Are Models for Cyberwar Preparation.
AN: 2629268
ISSN: 0016-3317

Record: 8
Title: Telecom links provide cyber-attack route.
Subject(s): AIR defenses—Yugoslavia; INFORMATION warfare—United States Source: Aviation Week & Space Technology, 11/08/99, Vol. 151 Issue 19, p81, 3p, 1c Author(s): Fulghum, David A.
Abstract: Reports on American military hackers' invasion of the computer that integrated the Yugoslav air defense system. Non-bombardment of Yugoslavia's telecommunication nodes during the summer 1999 campaign; Waging of information warfare (IW) to confuse and disable the Yugoslav air defense system; United States Air Force's modification of its EC-130 fleet with offensive electronic capabilities.
AN: 2523564
ISSN: 0005-2175

Record: 10
Title: To Fight Digitized or Analog.
Subject(s): INFORMATION warfare—United States; JOINT Readiness Training Center (Fort Polk, La.); NATIONAL Training Center (Fort Irwin, Calif.); FORTIFICATION—United States Source: Military Review, Nov/Dec99 Issue 6, p12, 6p, 1bw Author(s): Harris, III, James E.
Abstract: Compares the success in information dominance between the National Training Center in Fort Irwin, California and Joint Readiness Training Center in Fort Polk, Louisiana. Impact of battlespace and information dominance on command and control; Effect of information on command and control of a military force.
AN: 2742703
ISSN: 0026-4148

Record: 12
Title: The Future of War.
Subject(s): WAR; COUNCILS & synods—Russia (Federation); INFORMATION warfare; NON-governmental organizations; INTERNATIONAL police Source: Military Review, Nov/Dec99 Issue 6, p76, 2p Author(s): Bunker, Robert J.
Abstract: Reports the Ivan Bloch Commemorative Conference on the 'Future of War' held in St. Petersburg, Russia on February 24 to 27, 1999. Details on the organization of the conference; Expansion of the concept of information operations; Concern of nongovernment organizations on wars; Limitations of peacekeeping forces to deliver warfighting goals.
AN: 2742713
ISSN: 0026-4148

Record: 11
Title: Information Superiority and the Future of Mission Orders.
Subject(s): INFORMATION warfare—United States; UNITED States.—Army; UNITED States—Armed Forces; MILITARY missions; MILITARY art & science—Forecasting Source: Military Review, Nov/Dec99 Issue 6, p61, 7p, 4bw Author(s): Garrett, Anthony R.
Abstract: Suggests integrating information superiority with combined doctrine and mission orders to provide battle command for dominant maneuver in the United States (US) Armed Forces. Conditions for the US Army to retain centralized battle command; forecasts on lethal warfare in the 21st century.
AN: 2742710
ISSN: 0026-4148

Record: 13
Title: Information warfare highlights one of the most distressing weaknesses of COTS.
Subject(s): COMPUTER security; INFORMATION warfare; COMPUTER hackers
Source: Military & Aerospace Electronics, Oct99, Vol. 10 Issue 10, p14, 3p, 1c
Author(s): McHale
Abstract: Focuses on the weaknesses of commercial off-the-shelf computer and communications systems. Increased vulnerability of the systems to information warfare due to increased commonality with other systems; Threats of attack from hackers and techno-terrorists.
AN: 2525591
ISSN: 1046-9079

Record: 14
Title: Clinton to Request Immediate Funds For Info Security. (cover story)
Subject(s): INFORMATION warfare—United States; UNITED States.—National Security Council; COMPUTER security—United States
Source: Federal Times, 09/27/99, Vol. 35 Issue 34, p1, 2p, 2 charts, 1c
Author(s): Trimble, Stephen
Abstract: Reports on the plans of United States (US) President Bill Clinton's administration to ask the US Congress for funding to strengthen the government's defenses against cyber-attacks. Preparations of the US National Security Council for a fiscal 2000 supplementary budget request; Problem with computer security in US government agencies; Plans to create a volunteer force of computer students against computer attacks.
AN: 2307344
ISSN: 0014-9233

Record: 15
Title: Threat Convergence.
Subject(s): THREATS—United States; ESPIONAGE—United States; BUSINESS intelligence—United States; INFORMATION warfare—United States Source: Military Review, Sep/Oct99, Vol. 79 Issue 5, p2, 10p, 6bw Author(s): Flynt, Bill
Abstract: Focuses on the trend of threat convergence in the United States (US) in the 20th century. Reason for targeting the US population; Economic espionage and business intelligence in the country; Details on information warfare teams.
AN: 2651136
ISSN: 0026-4148

Record: 16
Title: Human Network Attacks.
Subject(s): PSYCHOLOGICAL warfare; INFORMATION warfare Source: Military Review, Sep/Oct99, Vol. 79 Issue 5, p23, 11p, 3bw Author(s): Thomas, Timothy L.
Abstract: Examines China's psychological warfare and knowledge concept and Russia's development of information-psychological operations. Chinese and Russian nontraditional military practices; Discussion on strategic culture and the information age; Concept weapons of China.
AN: 2651139
ISSN: 0026-4148

Record: 17
Title: Yugoslavia successfully attacked by computers. Subject(s): INFORMATION warfare—United States; COMPUTERS—United States; KOSOVO (Serbia) -- History—Civil War, 1998-Source: Aviation Week & Space Technology, 08/23/99, Vol. 151 Issue 8, p31, 2p, 1c Author(s): Fulghum, David A.
Abstract: Details the United States' use of offensive computer warfare during the Kosovo conflict in Serbia, Yugoslavia. Details of US efforts to penetrate Yugoslavia's military computers; Attempts to put false targets into the air defense system; Techniques explored in order to get into enemy computers.
AN: 2363060
ISSN: 0005-2175

Record: 19
Title: The Advent of Netwar: Analytic Background.
Subject(s): INFORMATION warfare; INFORMATION networks
Source: Studies in Conflict & Terrorism, Jul-Sep99, Vol. 22 Issue 3, p193, 14p
Author(s): Arquilla, John; Ronfeldt, David
Abstract: The information revolution is fostering the rise of network forms of organization, whereby small previously isolated groups can communicate, link up, and conduct coordinated joint actions as never before. This, in turn, is leading to a new mode of conflict—"netwar"—in which the protagonists depend on using network forms of organization, doctrine, strategy, and technology. Many actors across the spectrum of conflict—e.g., from ethno-nationalists, terrorists, and criminals who pose security threats, to social activists who do not—are developing netwar designs and capabilities. This article analyzes the rise of netwar, identifies the information-age behaviors that may characterize it, and discusses its varieties. [ABSTRACT FROM AUTHOR]
AN: 2223038
ISSN: 1057-610X

Record: 20
Title: Chechnya: A Glimpse of Future Conflict?
Subject(s): CHECHNIA (Russia) -- History—Civil War, 1994-; INFORMATION warfare—Russia (Federation) -- Chechnia
Source: Studies in Conflict & Terrorism, Jul-Sep99, Vol. 22 Issue 3, p207, 23p
Author(s): Arquilla, John; Karasik, Theodore
Abstract: Netwar, an emerging mode of conflict engaged in by networked, mostly nonstate actors is associated most with social activism (e.g., the Zapatistas), terror (e.g., bin Laden's Al Qaeda) and crime (e.g., the Asian triads). However, netwar can also manifest itself in highly militarized settings, particularly in the context of ethnonationalist conflict. The recent war in Chechnya provides a good example of how netwar can be used in extremely violent ways to confront and overcome the much larger conventional forces of nation-states. In this conflict, a network of clan-based Chechen fighters, organized in closely internetted small fighting cells, was able to defeat a valorous, but still-hierarchical, balky Russian army in the field. This case is also analytically important because the Chechens employed a wide range of netwar-oriented activities, from social activism to terror and strategic crime in order to complement their military netwar. [ABSTRACT FROM AUTHOR]
AN: 2223039
ISSN: 1057-610X

Record: 21
Title: Doctrinal Information Operations Issues.
Subject(s): INFORMATION warfare; MILITARY art & science Source: Military Intelligence Professional Bulletin, Jul-Sep99, Vol.25 Issue 3, p53, 3p, 3 charts
Abstract: Discusses the importance of information operations (IO) in military operations. Written documents on IO developed by the United States Armed Forces; Highlights on the techniques and procedures involved in IO; Integration of offensive and defensive operations in IO.
AN: 2315754
ISSN: 0026-4024

Record: 23
Title: Accidental/Inadvertent Nuclear War and Information Warfare. Subject(s): WAR; NUCLEAR disarmament; INFORMATION warfare Source: Armed Forces & Society, Summer99, Vol. 25 Issue 4, p653, 23p, 2 charts Author(s): Cimbala, Stephen J.
Abstract: Explains why the issue of nuclear deterrence and its possible relationship to information warfare, remains significant. Consideration of what must be done in order to guard against accidental/inadvertent nuclear war; Identification of some ways in which information warfare may increase the difficulty of accomplishing the said tasks necessary in the elimination of accidental/inadvertent war; Conclusions.
AN: 2336145
ISSN: 0095-327X

Record: 24
Title: IW Cyberlaw.
Subject(s): INFORMATION warfare—United States; INTERNATIONAL Telecommunications Satellite Organization; MILITARY art & science—
United States; SPACE law; CRIMINAL law—United States Source: Airpower Journal, Summer99, Vol. 13 Issue 2, p85, 18p, 3bw Author(s): Dicenso, David J.
Abstract: Focuses on treaties and laws governing information warfare (IW) in the United States. Definition of IW; Requirements for the resolution of the issue; Significance of space-related treaties;
Information on the International Telecommunications Satellite Organization Agreement; Application of criminal law on IW.
AN: 2111370
ISSN: 0897-0823

Record: 25
Title: EC-130Hs blanket Serb communications.
Subject(s): UNITED States.—Air Force; INFORMATION warfare—United States; BOMBING, Aerial—Yugoslavia; NORTH Atlantic Treaty Organization—Armed Forces
Source: Aviation Week & Space Technology, 05/03/99, Vol. 150 Issue 18, p30, 1p, 1c
Author(s): Wall, Robert
Abstract: Takes a look at the Operation Allied Force missions of three United States Air Force information warfare aircraft. Support for the North Atlantic Treaty Organization's air war against Yugoslavia; Goal of jamming Yugoslav military communications.
AN: 2077067
ISSN: 0005-2175

Record: 27
Title: Information Warfare.
Subject(s): INFORMATION warfare—United States; UNITED States—Defenses
Source: Popular Mechanics, Mar99, Vol. 176 Issue 3, p58, 4p, 6c, 1bw Author(s): WILSON, JIM; Blackman, Barry Abstract: Focuses on the information warfare attack capability of the United States. Series of hacks that has underscored vulnerability of US; Best defense against outside attack; Unit responsible for US attacks.
AN: 1547111
ISSN: 0032-4558

Record: 30
Title: Preventing Conflict Through Information Technology.
Subject(s): INFORMATION technology; INFORMATION warfare; PEACE—International cooperation; COMPUTER simulation
Source: Military Review, Dec98-Feb99, Vol. 78 Issue 6, p44, 14p, 5bw Author(s): Thomas, Timothy L.
Abstract: Focuses on information technology (IT) as a major conflict prevention tool and mechanism. Information on virtual peacemaking (VPM); Elements that can lead to warfare; Factors that make simulations vital in preparing the peace maker.
AN: 1917108
ISSN: 0026-4148

Record: 31
Title: Information operations go on the offensive.
Subject(s): INFORMATION warfare; UNITED States.—Joint Chiefs of Staff Source: Air Force Times, 11/23/98, Vol. 59 Issue 16, p30, 1/3p Author(s): Seffers, George I.
Abstract: Details the doctrine for conducting computer warfare adopted by the United States Joint Chiefs of Staff. Coverage of the documents on computer network attacks; Terminology used in the doctrine papers;
Issues on information operations.
AN: 1319222
ISSN: 0028-1697

Record: 32
Title: 'Joint doctrine' spurs information arms race.
Subject(s): INFORMATION warfare—United States; MILITARY doctrine—United States; UNITED States.—Joint Chiefs of Staff Source: Army Times, 11/23/98, Vol. 59 Issue 17, p26, 1/2p Author(s): Seffers, George I.

Abstract: Provides information on the doctrine for conducting information warfare being adopted by the Joint Chiefs of Staff of the United States. Implications of the move; What the doctrine paper includes; Explanations from several defense experts.

AN: 1318617
ISSN: 0004-2595

SWETSNETNAVIGATOR

INFORMATION WARFARE - Network Security Training Needed *Willingham, Stephen* National Defense - Journal of the American Defense Preparedness Association 2000 - volume 0 - issue 554 - page 31 - 32 :

CANADA - Information Warfare Research - The Department of National Defence is setting up a research team to study ways to track hackers and identify new types of computer viruses - Defense News 2000 - volume 15 - issue 11 - page 30

PREVIOUS ISSUES ALSO AVAILABLE FROM THE LIBRARY:

(MORE TITLES ARE AVAILABLE ON THE LIBRARY INTRANET SITE : HTTP://NT15B.HQ.NATO.INT/LIBRARY (MINERVA) OR HTTP://NT18/LIBRARY (EAPC)

No. 5/99	Ballistic Missiles
No. 8/99	Refugees and Migration Problems
No. 9/99	The Sanctions Dilemma
No. 2/00	The State of the Russian Economy
No. 3/00	The Baltic States
No. 4/00	The NPT since 1995
No. 5/00	NATO and the EAPC/PfP
No. 6/00	The European Security and Defence Identity/Policy (ESDI/P)

ANCIENS NUMEROS EGALEMENT DISPONIBLES A LA BIBLIOTHEQUE:

(D'AUTRES TITRES SONT ÉGALEMENT DISPONIBLES SUR LE SITE INTRANET DE LA BIBLIOTHÈQUE : HTTP://NT15B.HQ.NATO.INT/LIBRARY (MINERVA) OU HTTP://NT18/LIBRARY (CPEA)

No. 5/99	Les missiles ballistiques
No. 8/99	Les réfugiés et les problèmes de migration
No. 9/99	Les sanctions : un dilemme
No. 2/00	L'état de l'économie russe
No. 3/00	Les Etats Baltes
No. 4/00	Le TNP depuis 1995
No. 5/00	L'OTAN et le CPEA/PPP
No. 6/00	L'Identité/La Politique Européenne de Sécurité et de Défense (IESD/PESC)