NATO Library

THEMATIC BIBLIOGRAPHIES
NO. 7/2009

CYBER THREATS

LES CYBERMENACES

Bibliographies thématiques
No. 7/2009

Bibliothèque de l'OTAN

- **To contact us :**

  - NATO Library
    Public Diplomacy Division
    Room Nb123
    1110 Brussels
    Belgium
    Tel. : 32.2.707.44.14
    Fax : 32.2.707.42.49
    E-mail : library@hq.nato.int
  - *Intranet* : http://hqweb.hq.nato.int/oip/library/
  - *Internet* : http://www.nato.int/library

- **How to borrow items from the list below :**

  As a member of the NATO HQ staff you can borrow books (Type: M) for one month, journals (Type: ART) and reference works (Type: REF) for one week. Individuals not belonging to NATO staff can borrow books through their local library via the interlibrary loan system.

- **How to obtain the Library publications :**

  All Library publications are available both on the NATO Intranet and Internet websites.

- **Pour nous contacter :**

  - Bibliothèque de l'OTAN
    Division de la Diplomatie Publique
    Bureau Nb123
    1110 Bruxelles
    Belgique
    Tél. : 32.2.707.44.14
    Télécopieur : 32.2.707.42.49
    E-mail : library@hq.nato.int
  - *Intranet* : http://hqweb.hq.nato.int/oip/library/
  - *Internet* : http://www.nato.int/library

- **Comment emprunter les documents cités ci-dessous :**

  En tant que membre du personnel de l'OTAN vous pouvez emprunter les livres (Type: M) pour un mois, les revues (Type: ART) et les ouvrages de référence (Type: REF) pour une semaine. Les personnes n'appartenant pas au personnel d l'OTAN peuvent s'adresser à leur bibliothèque locale et emprunter les livres via le système de prêt interbibliothèques.

- **Comment obtenir les publications de la Bibliothèque :**

  Toutes les publications de la Bibliothèque sont disponibles sur les sites Intranet et Internet de l'OTAN.

PART I : BOOKS
*PREMIERE PARTIE : LIVRES**

2009

343 /00054 REF
Encyclopedia of Cybercrime - Westport, CT : Greenwood Press.
xxiii, 210 p.; 26 cm.
ISBN: 9780313339745
Subject(s):
1. COMPUTER CRIMES
Added entry(s):
1. MacQuade, Samuel C., ed.
Notes:
Bibliography: p. 195-200. Includes index.
'Cybercrime is not a new phenomenon, rather an evolving one with respect to adoption of information technology for abusive and criminal purposes. Further, by virtue of the myriad ways in which IT is abused, it represents a technological shift in the nature of crime rather than a new form of criminal behaviour. This work is the first comprehensive encyclopedia to address cybercrime. Topical articles address all key areas of concern and specifically those related to : terminology, definitions and social constructs of crime; national infrastructure security vulnerabilities and capabilities; types of attacks to computers and information systems; computer abusers and cybercriminals; criminological, sociological, psychological and technological theoretical underpinnings of cybercrime; social and economic impacts of crime enabled with information technology inclusive of harms experienced by victims of cybercrimes and computer abuse; emerging and controversial issues such as online pornography, the computer hacking subculture and potential negative effects of electronic gaming and so-called 'computer addiction'; and computer forensics as well as general investigation and prosecution of high tech crimes and attendant challenges around the world.'
ID number: 80022392
Year: 2009
Type: REF

323 /01103
Cyber Conflict and Global Politics - Abingdon, UK : Routledge.
xvi, 246 p.; 24 cm.
(Contemporary Security Studies)
ISBN: 9780415459709
Subject(s):
1. CYBERSPACE--POLITICAL ASPECTS
2. INTERNET--POLITICAL ASPECTS
3. POLITICAL VIOLENCE
Added entry(s):
1. Karatzogianni, Athina, ed.
Notes:
Bibliography: p. 212-237. Includes index.
'This volume examines theoretical and empirical issues relating to cyberconflict and its implications for global security and politics. Taking a multidimensional approach to current debates in Internet politics, the book comprises essays by leading experts from across the world. The volume includes a

* This list contains material received as of June 16th , 2009 – Cette liste est arrêtée au 16 juin 2009.

comprehensive introduction to current debates in the field and their ramifications for global politics, and follows this with empirical case studies. These include cyberconflict, cyberwars, information warfare and hacktivism, in contexts such as Sri Lanka, Lebanon and Estonia, the European Social Forum, feminist cyber crusades and the use of the Internet as a weapon by ethnoreligious and sociopolitical movements. The volume presents the theoretical debates and case studies of cyberconflict in a coherent, progressive and truly multidisciplinary way.'
ID number: 80022019
Year: 2009
Type: M

2007

343 /00051
Cybercriminalite : defi mondial et reponses - Paris : Economica.
viii, 281 p. : ill.; 24 cm.
ISBN: 9782717854459
Author(s):
1. Quenemer, Myriam
2. Ferry, Joel
Subject(s):
1. COMPUTER CRIMES
Notes:
'La lutte contre la cybercriminalite est un enjeu majeur pour le monde actuel. L'arsenal juridique doit constamment s'adapter a ces nouvelles formes de criminalite souvent d'envergure internationale qui exploitent les ressources des technologies numeriques comme objet d'infractions ou comme moyens pour faciliter la commission d'un crime ou d'un delit. Il apparaissait indispensable que soient reunis dans une meme etude a la fois les aspects techniques et juridiques de l'univers des reseaux numeriques ainsi que les reponses apportees a la derive de leurs utilisations. L'interet de cet ouvrage tient au regard tres averti et professionnel que les auteurs portent tant sur les multiples facettes de cette delinquance moderne et souvent organisee que sur les moyens mutualises pour la combattre. Forts de leur parcours de magistrate et de colonel de gendarmerie, ayant eu a connaitre de cette forme de criminalite tant au plan national qu'international, ils reussissent par leurs regards croises a faire partager leur passion pour la mise en oeuvre concrete et pertinente de la loi penale.'
ID number: 80021964
Year: 2007
Type: M

681 /00806
ICTs and International Security = Les technologies de l'information et la securite internationale - Geneva : UNIDIR.
52 + 58 p.; 30 cm.
(Disarmament Forum ; 3/07 = Forum du Desarmement ; 3/07)
Subject(s):
1. INFORMATION TECHNOLOGY--SECURITY MEASURES
2. COMPUTER NETWORKS--SECURITY MEASURES
3. COMPUTER SECURITY
4. CYBERTERRORISM
Added entry(s):
1. Vignard, Kerstin, ed.
2. Linekar, Jane, ed.
3. Compagnion, Valerie, ed.
4. United Nations Institute for Disarmament Research
Notes:
'This issue focuses on the civil and military threats posed by the

use of ICTs for military, terrorist and political purposes that run counter to the maintenance of international security, and which could cause serious political, social and economic consequences. In order to encourage discussion, a wide range of perspectives on topics related to information security are presented. These include legal aspects of cyberspace and information warfare as they relate to national and international security; a discussion of cyberterrorism and Internet governance issues; how risks to critical information infrastructure can be analysed; and how various international and regional forums are addressing particular aspects of the information security issue.'

ID number: 80021584
Year: 2007
Type: M

2006

323 /01017
Terror on the Internet : The New Arena, the New Challenges - Washington : United States Institute of Peace Press.
xv, 309 p.; 24 cm.
ISBN: 9781929223718
Author(s):
1. Weimann, Gabriel, 1950-
Subject(s):
1. TERRORISM--COMPUTER NETWORK RESOURCES
2. CYBERTERRORISM
3. CYBERTERRORISM--PREVENTION
Notes:
Includes index.
'The author reveals here that terrorist organizations and their supporters maintain hundreds of web sites, taking advantage of the unregulated, anonymous, and accessible nature of the Internet to target an array of messages to diverse audiences. Drawing on an eight-year study of the World Wide Web, the author examines how modern terrorist organizations exploit the Internet to raise funds, recruit members, plan and launch attacks, and publicize their chilling results. He also investigates the effectiveness of counterterrorism measures, and warns that this cyberwar may cost us dearly in terms of civil rights.'

ID number: 80021318
Year: 2006
Type: M

2004

323 /00871
Cyberterrorism - Aldershot, UK : Ashgate.
xix, 312 p.; 25 cm.
(The International Library of Essays in Terrorism)
ISBN: 0754624269
Subject(s):
1. CYBERTERRORISM
Added entry(s):
1. O'Day, Alan, ed.
Notes:
Includes index.
'The 22 essays republished in this volume assess a number of the germane issues surrounding cyberterrorism - its substance, why it is attractive to terrorists, the legal problems involved countering it, prospects for international cooperation, means of defending against cyberattacks and the outlook for the future.'

ID number: 80019745

Year: 2004
Type: M

2003

681 /00810
Protecting Critical Infrastructures Against Cyber-Attack - Oxford, UK : Oxford University Press.
98 p. : ill.; 24 cm.
(Adelphi paper, 0567-932X ; 359)
ISBN: 0198530161
Author(s):
1. Lukasik, Stephen J.
2. Goodman, Seymour E.
3. Longhurst, David W.
Subject(s):
1. INFRASTRUCTURE (ECONOMICS)--SECURITY MEASURES
2. CYBERTERRORISM--PREVENTION
3. INFORMATION SUPERHIGHWAY--SECURITY MEASURES
4. COMPUTER SECURITY
5. COMPUTER NETWORKS--SECURITY MEASURES
Added entry(s):
1. International Institute for Strategic Studies (GB)
Notes:
'Advances in information technologies and their adoption in all sectors of modern life are not problem-free. This study examines the negative impact of those technologies on the central infrastructure systems on which societies depend for the delivery of essential services such as communication, electric power, transportation, and on the information systems that enable governments to function and economic enterprises to flourish. The underlying technologies of networked computer hardware and software are susceptible to massive failure. But unlike physical networks that can be engineered to be robust against natural events, random failures and even local sabotage, information systems are particularly susceptible to malicious acts. Attacks can exploit the connections that are a major virtue and failures in one part can propagate widely. This global character of information system vulnerabilities constitutes severe challenges to both national governments and the private owners of such critical systems. This paper examines the national strategies designed to cope with the emerging societal vulnerabilities and offers appropriate roles for both public and private sectors.'
ID number: 80019178
Year: 2003
Type: M

2001

355.4 /01348
Networks and Netwars : The Future of Terror, Crime, and Militancy - Santa Monica, CA : Rand Corporation.
xiv, 375 p. : ill.; 23 cm.
ISBN: 0833030302
Subject(s):
1. NETWAR
2. CYBERTERRORISM
3. INFORMATION WARFARE
Added entry(s):
1. Arquilla, John, ed.
2. Ronfeldt, David F., ed.
3. Rand Corporation (US)
Notes:
'Netwar is the lower-intensity, societal-level counterpart to our earlier, mostly military concept of cyberwar. Netwar has a dual

nature, in that it is composed of conflicts waged, on the one hand, by terrorists, criminals, and ethnonationalist extremists; and by civil-society activists on the other. What distinguishes netwar as a form of conflict is the networked organizational structure of its practitioners - with many groups actually being leaderless - and the suppleness in their ability to come together quickly in swarming attacks. The concepts of cyberwar and netwar encompass a new spectrum of conflict that is emerging in the wake of the information revolution. This volume studies major instances of netwar that have occurred over the past several years and finds, among other things, that netwar works very well. In part, the success of netwar may be explained by its very novelty - much as earlier periods of innovation in military affairs have seen new practices triumphant until an appropriate response is discovered. But there is more at work here : the network form of organization has reenlivened old forms of licit and illicit activity, posing serious challenges to those - mainly the militaries, constabularies, and governing officials of nation states - whose duty is to cope with the threats this new generation of largely nonstate actors poses.'

ID number: 80018284
Year: 2001
Type: M

2000

355.4 /01601
Transnational Threats : Blending Law Enforcement and Military Strategies - Carlisle Barracks, PA : US Army War College.
vii, 256 p.; 23 cm.
ISBN: 1584870370
Subject(s):
1. CYBERTERRORISM
2. WMD TERRORISM
3. COMPUTER CRIMES
4. ORGANIZED CRIME
5. USA--NATIONAL SECURITY
6. LAW ENFORCEMENT--USA
7. INFORMATION WARFARE

Added entry(s):
1. US Army War College. Strategic Studies Institute (US)

Notes:
'On February 2-3, 2000, the US Army War College, the Triangle Institute for Security Studies, and the Duke University Center for Law, Ethics, and National Security co-sponsored a conference in Chapel Hill, North Carolina. The conference examined transnational threats, including terrorism involving weapons of mass destruction, cyber threats to the national infrastructure, and international organized crime. The goal was to evaluate the seriousness of such threats and discuss strategies for dealing with them. In particular, the conference sought to address the question of how military and law enforcement could blend their strategies to better counter transnational threats. A secondary purpose was to clarify the role of the military in meeting challenges that transcend national borders and threaten our national interests. This book highlights some of the main issues and themes that ran through the conference. After looking at the various threats and undertaking a risk assessment, the book considers the unique aspects of transnational threats, and then identifies the key challenges facing the US, paying particular attention to the role of the military. To conclude, the book discusses some of the steps that should be taken to secure ourselves against transnational threats.'

ID number: 80017080
Year: 2000

Type: M

1998

323 /00629
Technology and Terrorism : The New Threat for the Millennium - Leamington Spa, UK : RISCT.
24 p.; 25 cm.
(Conflict studies, 0069-8792 ; 309)
Author(s):
1. Bowers, Stephen R.
2. Keys, Kimberly R.
Subject(s):
1. CYBERTERRORISM
Added entry(s):
1. Research Institute for the Study of Conflict and Terrorism (GB)
Notes:
'The end of the 20th century may have seen a decline in the number of incidents of 'traditional' terrorism such as hijackings and kidnappings but the lethality of the terrorist potential has risen to a frightening degree with the advent of cyberterrorism, and its links to computer technology. Access to new terrorist tools, the broadening of the terrorist market, and the advent of sophisticated and readily available information technologies are all significant factors. In this highly topical study the authors examine the new terrorist tools and their appalling capacity for the destruction of human systems. Together with chemical and biological terrorism, the 'silent invaders' of computer technology are the new threat for the millennium. The authors claim that the technological revolution has effectively 'democratised' computer knowledge so that the forces of law and order no longer have an inherent advantage of power and privilege. Their special challenge in the new century will be to match the resourcefulness and ingenuity of their terrorist adversaries.'
ID number: 80014853
Year: 1998
Type: M

681 /00811
Les cyberconflits : Internet, autoroutes de l'information et cyberspace : quelles menaces ? - Bruxelles : GRIP.
102 p. : ill.; 21 cm.
(Publications du GRIP ; 228)
ISBN: 2870277113
Author(s):
1. Wautelet, Michel
Subject(s):
1. CYBERSPACE
2. COMPUTER CRIMES
3. INFORMATION WARFARE
4. CYBERTERRORISM
5. INFORMATION SUPERHIGHWAY
6. INTERNET
Added entry(s):
1. Institut Europeen de Recherche et d'Information sur la Paix et la Securite (BE)
Notes:
'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 ?'

ID number: 80014781
Year: 1998
Type: M

1996

681 /00781
Security in Cyberspace : Challenges for Society - Santa Monica, CA : Rand Corporation.
xiii, 59 p.; 28 cm.
(Rand Conference Proceedings ; CF-128-RC)
ISBN: 0833024701
Subject(s):
1. COMPUTER SECURITY
2. COMPUTER NETWORKS--SECURITY MEASURES
3. INFRASTRUCTURE (ECONOMICS)--SECURITY MEASURES
4. INFORMATION SUPERHIGHWAY--SECURITY MEASURES
5. CYBERTERRORISM--PREVENTION

Added entry(s):
1. Rand Corporation (US)
2. Ditchley Foundation (GB)

Notes:
Proceedings of an International Conference.
Bibliography: p. 59.
'On April 26-28, 1996, Rand Corporation and the Ditchley Foundation jointly sponsored an international conference in Santa Monica, California to discuss 'Security in Cyberspace: Challenges for Society'. This conference brought together a group of senior-level North American and European intellectual leaders from the many communities impacted by and with a role to play in cyberspace security. Topics covered include the magnitude of the cyberspace security threat and the threat's consequences; impediments to improved security in cyberspace and what must be done to remove them; and means to achieve international cooperation regarding security in cyberspace.'

ID number: 80017467
Year: 1996
Type: M

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

2009

Cybercriminalite, cyberconflits.
(DEFENSE NATIONALE ET SECURITE COLLECTIVE, 65e annee, no. 3, mars 2009, numero entier.)
Subject(s):
1. COMPUTER CRIMES
2. CYBERTERRORISM
ID Number: JA025699
Year: 2009
Language: French
Type: ART

Digital Defences.
(WORLD TODAY, vol. 65, no. 4, April 2009, p.19-21.)
Author(s):
1. Hughes, Rex
Subject(s):
1. COMPUTER CRIMES--PREVENTION--NATO
2. CYBERTERRORISM--PREVENTION--NATO
Notes:
As NATO celebrates its sixtieth anniversary, it is worth considering to what extent the 26-member alliance has evolved since its founding. While ostensibly convened to defend Western Europe against a full scale Soviet military invasion or nuclear attack, the underlying mission of the world's premier military alliance has changed dramatically since the end of the Cold War. Now operating 'out of area' in Afghanistan, it has also had to confront the difficulties of operating in a totally different borderless realm.
ID Number: JA025749
Year: 2009
Language: English
Type: ART

Al-Qaida's Virtual Crisis.
(RUSI JOURNAL, vol. 154, no. 1, February 2009, p. 56-64.)
Author(s):
1. Awan, Akil N.
2. Al-Lami, Mina
Subject(s):
1. QAIDA (ORGANIZATION)
2. JIHAD
3. TERRORISM--COMPUTER NETWORK RESOURCES
Notes:
The fight Al-Qa'ida has waged against the West has been fought on a virtual as well as physical battlefield. Recently, many jihadist strongholds and hiding places on the web have been shut down. This article charts the growth and the current crisis of Al-Qa'ida's 'media jihad'.
ID Number: JA025649
Year: 2009
Language: English
Type: ART

** This list contains material received as of June 16th , 2009 – Cette liste est arrêtée au 16 juin 2009.

Regulating the 'Dark Web' : How a Two-Fold Approach can Tackle Peer-to-Peer Radicalisation.
(RUSI JOURNAL, vol. 154, no. 2, April 2009, p. 28-33.)
Author(s):
1. Stevens, Tim
Subject(s):
1. TERRORISM--COMPUTER NETWORK RESOURCES
2. JIHAD
3. INTERNET--LAW AND LEGISLATION
Notes:
The Internet plays a contributory role in radicalisation, but it is only a number of mechanisms currently deployed to win recruits to global jihad. Technical regulation of online content is difficult and may be counter-productive, driving forums deeper underground or alienating users. The author argues that adopting a social approach that educates and empowers online communities could have more success.
ID Number: JA025818
Year: 2009
Language: English
Type: ART

2008

Conflit Georgie-Russie : Internet, l'autre champ de bataille.
(DEFENSE NATIONALE ET SECURITE COLLECTIVE, 64e annee, no. 10, octobre 2008, p. 51-56.)
Author(s):
1. Ifrah, Laurence
Subject(s):
1. GEORGIA (REPUBLIC)--FOREIGN RELATIONS--SOUTH OSSETIA (GEORGIA)
2. SOUTH OSSETIA (GEORGIA)--FOREIGN RELATIONS--GEORGIA (REPUBLIC)
3. GEORGIA (REPUBLIC)--FOREIGN RELATIONS--RUSSIA (FEDERATION)
4. RUSSIA (FEDERATION)--FOREIGN RELATIONS--GEORGIA (REPUBLIC)
5. SOUTH OSSETIA (GEORGIA)--HISTORY--AUTONOMY AND INDEPENDENCE MOVEMENTS
6. COMPUTER CRIMES
7. CYBERTERRORISM
Notes:
Dans le conflit arme entre la Georgie, l'Ossetie du Sud et la Russie, des attaques informatiques ont ete perpetrees principalement a l'encontre des sites georgiens mais aussi des serveurs russes et ossetes. Suivis de pres par les experts en securite des systemes d'information, ces assauts ont parfois donne lieu a des interpretations fantaisistes dues au fait qu'il est techniquement impossible de prouver quels sont les auteurs de ces mefaits. Certains d'entre eux s'inspirant d'ecrits douteux circulant sur la toile se sont empresses de commenter ces evenements sans malheureusement prendre la peine de verifier leurs sources. Les nombreuses informations publiees sur ce conflit demontrent a quel point il est facile de se laisser manipuler par des personnes que les interets politiques poussent a la desinformation et a la propagande.
ID Number: JA025193
Year: 2008
Language: French
Type: ART

Cyberespace : le nouveau defi des Etats, entre cyberconflit et cybercriminalite.
(DEFENSE NATIONALE ET SECURITE COLLECTIVE, 64e annee, no. 12, decembre 2008, p. 115-128.)
Author(s):
1. Ifrah, Laurence
Subject(s):
1. COMPUTER CRIMES
2. CYBERSPACE
Notes:
Nouveau champ de bataille, le cyberespace, theatre d'attaques numeriques est a la fois source de fascination et de fantasmes. Les moyens mis en oeuvre pour assurer defense et riposte suscitent de nombreuses interrogations du fait du manque de visibilite sur les points strategiques que constituent l'identite des auteurs des attaques et les ressources tant humaines que materielles dont dispose l'Etat. La prise de conscience des menaces par tous les acteurs, Etat, entreprises, particuliers est loin d'etre acquise.
ID Number: JA025417
Year: 2008
Language: French
Type: ART

De la cybercriminalite a la cyberguerre.
(DEFENSE NATIONALE ET SECURITE COLLECTIVE, 64e annee, no. 5, mai 2008 (plusieurs articles).)
Subject(s):
1. COMPUTER CRIMES
ID Number: JA024884
Year: 2008
Language: French
Type: ART

Web War I : Is Europe's First Information War a New Kind of War ?.
(COMPARATIVE STRATEGY, vol. 27, no. 3, 2008, p. 227-247.)
Author(s):
1. Blank, Stephen
Subject(s):
1. COMPUTER CRIMES--ESTONIA
2. CYBERTERRORISM--ESTONIA
Notes:
In April-May 2007, Estonia experienced several weeks of coordinated cyberattacks against its financial and sociopolitical institutions. Although the origin of these attacks cannot be definitively named, it is widely believed in Estonia and among many analysts that Moscow was behind these attacks. Certainly these attacks represented the culmination of plans set in motion a year earlier to attack the Estonian government and society for their supposedly anti-Russian policies. And the accompanying demonstrations in Tallinn at this time also represented well-worn Soviet techniques used in earlier coups in Eastern Europe. Ultimately the advent of such new forms of military operations confirms a threat assessment by which any one operation on land, sea, air, underwater, or space can target anyone in any of these dimensions and raises provocative issues for both analysts of war and government officials.
ID Number: JA025076
Year: 2008
Language: English
Type: ART

How Did Europe's Global Jihadis Obtain Training for Their Militant Causes ?.
(TERRORISM AND POLITICAL VIOLENCE, vol. 20, no. 2, April - June 2008, p. 234-256.)
Author(s):
1. Nesser, Petter
Subject(s):
1. TERRORISTS--TRAINING OF--EUROPE
2. TERRORISM--COMPUTER NETWORK RESOURCES
3. JIHAD
Notes:
This article examines, compares amd contrasts the ways in which 'global jihadis' have trained for terrorism in Western Europe. Before the invasion of Afghanistan, the terrorists received training in Al Qaeda paramilitary camps. After invasion, they had to find alternative training methods and arenas. It is widely assumed that the Internet has taken over the role of the Afghan camps. The current survey suggests that the Internet's role as a 'virtual training camps' might be overstated. Although the Net has become an important tool for terrorists on many levels, they maintain an urge to obtain real-life, military-style training in jihadi combat zones. Despite difficulties and risks, many of today's terrorists attend terrorist training facilities in Pakistan and other places. The main characteristic of training practices after the invasion of Afghanistan seems to be that, from an organizational perspective, the push for training and preparation comes from 'below' rather than 'above'.
ID Number: JA024930
Year: 2008
Language: English
Type: ART

The Internet : A Virtual Training Camp.
(TERRORISM AND POLITICAL VIOLENCE, vol. 20, no. 2, April - June 2008, p. 215-233.)
Author(s):
1. Stenersen, Anne
Subject(s):
1. TERRORISTS--TRAINING OF
2. TERRORISM--COMPUTER NETWORK RESOURCES
3. QAIDA (ORGANIZATION)
Notes:
This study aims to investigate how Al Qaeda uses the Internet for military training and preparation. What kind of training is available on jihadi webpages, who produces it, and for what purpose ? The article argues that in spite of a vast amount of training-related literature online, there have been few organized efforts by Al Qaeda to train their followers by way of the Internet. The Internet is per today not a 'virtual training camp', organized from above, but rather a resource bank maintained and accessed by self-radicalized sympathizers.
ID Number: JA024929
Year: 2008
Language: English
Type: ART

2007

Cyberconflits : vers la premiere cyberguerre.
(DEFENSE NATIONALE ET SECURITE COLLECTIVE, 63eme annee, no. 11, novembre 2007, p. 153-159.)
Author(s):
1. Ifrah, Laurence
Subject(s):
1. CYBERTERRORISM
2. COMPUTER CRIMES
Notes:
Depuis quelques mois, les systemes d'information des pays occidentaux sont victimes d'attaques virulentes provenant de la RPC (Republique populaire de Chine). Organisees ou non par l'Armee populaire de liberation de la Chine (APL), il n'y a aucun doute sur le fait qu'elle proviennent de pirates informatiques (hackers) de haut niveau qui ont beneficie de moyens techniques et financiers importants completes par des informations precises sur les infrastructures de leurs cibles. Ces intrusions sont complexes a mettre en oeuvre et ne peuvent s'improviser, il est beaucoup plus complique de lancer une attaque dans le but de recuperer de l'information a caractere confidentiel voire classifie, que de detruire des serveurs ennemis comme cela avait ete le cas pour l'Estonie.
ID Number: JA024215
Year: 2007
Language: French
Type: ART

Terrorist Use of the Internet : The Real Story.
(JOINT FORCE QUARTERLY, no. 45, 2007, p. 100-103.)
Author(s):
1. Lachow, Irving
2. Richardson, Courtney
Subject(s):
1. CYBERTERRORISM
2. TERRORISM--COMPUTER NETWORK RESOURCES
Notes:
This article examines why the Internet is so useful for terrorist organizations. It then considers how terrorists use the Internet for strategic advantage and why the threat of cyberterrorism may be overstated in many cases. The article concludes with a set of observations and recommendations.
ID Number: JA023495
Year: 2007
Language: English
Type: ART

Radicalization on the Internet ? The Virtual Propagation of Jihadist Media and Its Effects.
(RUSI JOURNAL, vol. 152, no. 3, June 2007, p. 76-81.)
Author(s):
1. Awan, Akil N.
Subject(s):
1. JIHAD
2. TERRORISM--COMPUTER NETWORK RESOURCES
ID Number: JA023864
Year: 2007
Language: English
Type: ART

2006

The Real Online Terrorist Threat.
(FOREIGN AFFAIRS, vol. 85, no. 5, September - October 2006, p. 115-134.)
Author(s):
1. Kohlmann, Evan F.
Subject(s):
1. TERRORISM--COMPUTER NETWORK RESOURCES
Notes:
Fears of a 'digital Pearl Harbor' - a cyberattack against critical infrastructure - have so preoccupied Western governments that they have neglected to recognize that terrorists actually use the Internet as a tool for organizing, recruiting, and fundraising. Their online activities offer a window onto their methods, ideas, and plans.
ID Number: JA022824
Year: 2006
Language: English
Type: ART

2005

Cyber War und Cyber Terrorismus als neue Formen des Krieges.
(OSTERREICHISCHE MILITARISCHE ZEITSCHRIFT, 43. Jg., Heft 2, Marz - April 2005, S. 203-211.)
Author(s):
1. Unger, Walter F.
2. Vetschera, Heinz
Subject(s):
1. CYBERTERRORISM
2. NETWORK CENTRIC WARFARE
3. INFORMATION WARFARE
ID Number: JA021314
Year: 2005
Language: German
Type: ART

Cyberterrorism : The Sum of All Fears ?.
(STUDIES IN CONFLICT AND TERRORISM, vol. 28, no. 2, March - April 2005, p. 129-149.)
Author(s):
1. Weimann, Gabriel
Subject(s):
1. CYBERTERRORISM
Notes:
Cyberterrorism conjures up images of vicious terrorists unleashing catastrophic attacks against computer networks, wreaking havoc, and paralyzing nations. This is a frightening scenario, but how likely is it to occur ? Could terrorists cripple critical military, financial, and service computer systems ? This article charts the rise of cyberangst and examines the evidence cited by those who predict imminent catastrophe. Psychological, political, and economic forces have combined to promote the fear of cyberterrorism. From a psychological perspective, two of the greatest fears of modern time are combined in the term 'cyberterrorism'. The fear of random, violent victimization segues well with the distrust and outright fear of computer technology. Many of these fears, the report contends, are exaggerated : not a single case of cyberterrorism has yet been recorded, hackers are regularly mistaken for terrorists, and cyberdefenses are more robust than is commonly supposed. Even so, the potential threat is undeniable and seems likely to increase, making it all the more important to address the

danger without inflating or manipulating it.
ID Number: JA021395
Year: 2005
Language: English
Type: ART

2004

Bangs for the Buck : A Cost-Benefit Analysis of Cyberterrorism.
(STUDIES IN CONFLICT AND TERRORISM, vol. 27, no. 5, September - October 2004, p. 387-408.)
Author(s):
1. Giacomello, Gianpiero
Subject(s):
1. CYBERTERRORISM
Notes:
Just like 'the Internet', the word 'terrorism' has become an icon of the times. If the two terms are combined 'cyberterrorism' emerges, along with an endless list of gloomy scenarios. Is this outcome really unavoidable ? Would cyberterrorism be a viable option for terrorists ? This article addresses these questions assuming that a hypothetical terrorist group, interested in adding cyberterrorism to its arsenal, decides to engage in a cost-benefit analysis to assess the payoffs and investment required by such a new endeavor. The conclusions are that cyberterrorism is not a very efficient substitute for more traditional tools like bombs. It is more effective for the terrorists to exploit information infrastructures to fight a 'war of ideas', spreading their beliefs and points of view.
ID Number: JA020931
Year: 2004
Language: English
Type: ART

Terrorism and Mass Communication : Nitro to the Net.
(WORLD TODAY, vol. 60, no. 8 - 9, August - September 2004, p. 19-22.)
Author(s):
1. Conway, Maura
Subject(s):
1. TERRORISM--COMPUTER NETWORK RESOURCES
ID Number: JA020791
Year: 2004
Language: English
Type: ART

2003

La menace deterritorialisee et desetatisee : le cyberconflit.
(REVUE INTERNATIONALE ET STRATEGIQUE, no. 49, printemps 2003, p. 165-171.)
Author(s):
1. Stella, Marie
Subject(s):
1. CYBERTERRORISM
2. COMPUTER CRIMES
Notes:
La derniere decennie a ete le theatre de bouleversements sans precedent avec l'emergence et le developpement rapide des nouvelles technologies de l'information et de la communication. Cette revolution a confere une dimension strategique a la protection des reseaux et des systemes d'information. L'un des paradoxes de la richesse de la societe d'information et de son haut degre de developpement technologique est de creer des vulnerabilites au coeur meme de ces systemes d'information. Le cyberespace offre alors un cadre privilegie aux individus et

aux groupes organises animes d'intentions criminelles, qui echappent a toute contingence de lieu et de temporalite.
ID Number: JA018976
Year: 2003
Language: French
Type: ART

Al Qaeda and the Internet : The Danger of 'Cyberplanning'.
(PARAMETERS, vol. 33, no. 1, Spring 2003, p. 112-123.)
Author(s):
1. Thomas, Timothy L.
Subject(s):
1. CYBERTERRORISM--PREVENTION
2. TERRORISM--COMPUTER NETWORK RESOURCES
Notes:
The author explores the possibility of the Internet as a 'cyberplanning' tool for terrorists. Based on evidence that the Internet was used by al Qaeda in its planning for 9/11 and recent military uses by various governments, Thomas believes the Internet is, in part, a digital menace. It provides terrorists (and governments) with anonymity, command and control resources, and a host of other measures to coordinate and integrate attack options. The author offers 16 measures that law enforcement agencies might consider in detecting terrorists' methodologies on the Internet. He concludes that if law enforcement and government agencies 'cyberplan' properly, we can counter the use of the Internet by cyberterrorists and hostile nations.
ID Number: JA019180
Year: 2003
Language: English
Type: ART

2002

Internet Warfare in the Middle East : Cyberwar.
(WORLD TODAY, vol. 58, no. 4, April 2002, p. 7-8.)
Author(s):
1. Trendle, Giles
Subject(s):
1. CYBERTERRORISM
2. COMPUTER CRIMES
Notes:
With the escalation of violence in Israel and the occupied territories comes concern about a less visible threat - a second Arab-Israeli cyberwar. Possible scenarios include the release of viruses that could infect computer systems worldwide and hacker attacks on the databases of western businesses and public utility networks.
ID Number: JA017646
Year: 2002
Language: English
Type: ART

What is Cyberterrorism ?.
(CURRENT HISTORY, vol. 101, no. 659, December 2002, p. 436-442.)
Author(s):
1. Conway, Maura
Subject(s):
1. CYBERTERRORISM
Notes:
Are terrorist groups who operate in cyberspace 'cyberterrorists' ? The answer hinges on what constitutes cyberterrorism. Admittedly, terrorism is a notoriously difficult concept to define; however, the addition of computers to old-fashioned criminality is not.
ID Number: JA018713
Year: 2002
Language: English
Type: ART

Cyberterrorism Hackers Threaten Suicide Attacks.
(WORLD TODAY, vol. 58, no. 11, November 2002, p. 10-11.)
Author(s):
1. Trendle, Giles
Subject(s):
1. CYBERTERRORISM
Notes:
Could war against Iraq provoke digital counterattacks from hackers around the world, or is talk of cyberterrorism just hysteria whipped up by fearmongers with their own agendas ?
ID Number: JA018444
Year: 2002
Language: English
Type: ART

www.terrorism.com : Terror on the Internet.
(STUDIES IN CONFLICT AND TERRORISM, vol. 25, no. 5, 2002, p. 317-332.)
Author(s):
1. Tsfati, Yariv
2. Weimann, Gabriel
Subject(s):
1. TERRORISM--COMPUTER NETWORK RESOURCES
Notes:
The nature of the Internet - the ease of access, the chaotic structure, the anonymity, and the international character - all furnish terrorist organizations with an easy and effective arena for action. The present research focuses on the use of the Internet by modern terrorist organizations and attempts to describe the uses terrorist organizations make of this new communication technology. Is the use of the Internet by terrorists different from that of other, 'conventional' means of communication ? How can governments respond to this new challenge ? The population examined in this study is defined as the Internet sites of terrorist movements as found by a systematic search of the Internet, using various search engines. The sites were subjected to a qualitative content analysis, focusing on their rhetorical structures, symbols, persuasive appeals, and communication tactics. The study reveals differences and similarities between terrorist rhetoric online and in the conventional media.
ID Number: JA018375
Year: 2002
Language: English
Type: ART

2001

La guerra cibernetica.
(POLITICA EXTERIOR, vol. 15, no. 80, marzo - abril 2001, p. 131-149.)
Author(s):
1. Wegener, Henning
Subject(s):
1. INFORMATION WARFARE
2. CYBERTERRORISM
3. COMPUTER CRIMES
4. CYBERTERRORISM--PREVENTION
5. COMPUTER CRIMES--PREVENTION
Notes:
Las tecnologicas de la informacion han llegado tambien a la esfera de la seguridad. En un fenomeno que no conce fronteras, la defensa nacional requiere estrategias y medios para prevenir y afrontar ataques ciberneticos. La cooperacion multilateral y las legislaciones nacionales problamente sean insuficientes para actuar contra delitos de esta naturaleza.
ID Number: JA016444
Year: 2001
Language: Spanish
Type: ART

The Ethics of Computer Network Attack.
(PARAMETERS, vol. 31, no. 1, Spring 2001, p. 44-58.)
Author(s):
1. Bayles, William J.
Subject(s):
1. CYBERTERRORISM
Notes:
The author examines the ethics associated with attacks in cyberspace. He attempts to adjudicate between factions arguing that computer network attack does not even qualify as a use of force and those believing such actions equate to attack with weapons of mass destruction. A doctrine and strategy must be developed, he concludes, that will permit the US to police this dimension as well as defend our national interests.
ID Number: JA016276
Year: 2001
Language: English
Type: ART

2000

From Car Bombs to Logic Bombs : The Growing Threat from Information Terrorism.
(TERRORISM AND POLITICAL VIOLENCE, vol. 12, no. 2, Summer 2000, p. 97-122.)
Author(s):
1. Post, Jerrold M.
2. Ruby, Keven G.
3. Shaw, Eric D.
Subject(s):
1. CYBERTERRORISM
Notes:
The vulnerability of the critical infrastructure has led to increasing concern that it will be the target of terrorist attacks. This article explores definitional aspects of information terrorism and identifies two groups likely to find information terrorism attractive : conventional terrorism groups and information culture groups. As computer sophisticated youth move into the ranks of conventional terrorism groups, the groups will increase their reliance on

computer technology, and information terrorism will be incorporated into a hybrid tactical repertoire. Information culture groups, however, confine their attacks to cyberspace. In contrast to the powerful group dynamics of the traditional underground terrorist group, networked groups, particularly information culture terrorists, may only be in contact electronically, and are subject to a radically different group psychology, 'virtual group dynamics', that significantly affects their decision making and risk taking, and has dangerous security implications.

ID Number: JA016085
Year: 2000
Language: English
Type: ART

Affecting Trust : Terrorism, Internet and Offensive Information Warfare.
(TERRORISM AND POLITICAL VIOLENCE, vol. 12, no. 1, Spring 2000, p. 15-36.)
Author(s):
1. Valeri, Lorenzo
2. Knights, Michael
Subject(s):
1. CYBERTERRORISM
Notes:
The national security consequences of the potential use of the Internet by terrorist organizations have attracted the interest of many academics and government and intelligence officials. The goal of this article is to provide a new explanatory angle concerning the possible targets of terrorists' offensive information warfare (OIW) operations. It argues that these organizations may prove more valuable and effective to undermine on-line activities of leading electronic commerce sites than to target elements of the critical national information infrastructure. These offensive actions, in fact, would directly impact one of the explanatory elements for the Internet's success : users' perception of its trustworthiness. Before tackling its arguments, the article provides a definition of offensive information warfare. Then, it investigates how terrorist organizations would formulate their operational style concerning offensive information warfare. The stage is then set to define the central argument of the article by drawing from studies carried out in the areas of information security, international management and electronic commerce. The article concludes with a set of policy recommendations to counter these potential threats and thus make the Internet a safer communication instrument for economic, commercial and social development.

ID Number: JA015425
Year: 2000
Language: English
Type: ART

Cyber-attacks and International Law.
(SURVIVAL, vol. 42, no. 3, Autumn 2000, p. 89-103.)
Author(s):
1. Grove, Gregory D.
2. Goodman, Seymour E.
3. Lukasik, Stephen J.
Subject(s):
1. CYBERTERRORISM--PREVENTION
Notes:
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.
ID Number: JA015614
Year: 2000
Language: English
Type: ART

1997

Cyber-terrorisme : le nouveau peril.
(POLITIQUE INTERNATIONALE, no. 77, automne 1997, p. 299-312.)
Author(s):
1. Martin, Daniel
Subject(s):
1. CYBERTERRORISM
2. COMPUTER CRIMES
Notes:
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.
ID Number: JA012347
Year: 1997
Language: French
Type: ART

Cyber-Terrorism : The Shape of Future Conflict.
(RUSI JOURNAL, vol. 142, no. 5, October 1997, p. 40-45.)
Author(s):
1. Rathmell, Andrew
Subject(s):
1. INFORMATION WARFARE
2. CYBERTERRORISM
Notes:
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.
ID Number: JA012290
Year: 1997
Language: English
Type: ART

Previous Issues

No. 1/09	Management
No. 2/09	The Cold War
No. 3/09	NATO's 23rd Summit Meeting in Strasbourg/Kehl
No. 4/09	The Taliban
No. 5/09	North Korea's Nuclear Weapons Programme
No. 6/09	Irregular Warfare

Anciens numéros

No. 1/09	Le management
No. 2/09	La guerre froide
No. 3/09	Le 23ème sommet de l'OTAN à Strasbourg/Kehl
No. 4/09	Les Taliban
No. 5/09	Le programme d'armes nucléaires de la Corée du Nord
No. 6/09	La guerre irrégulière