Cyberterrorism

Articles :

The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge
11th Annual International Symposium on Criminal Justice Issues
Barry C. Collin, Institute for Security and Intelligence
Available online at: *http://afgen.com/terrorism1.html*

Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy
Dorothy E. Denning, Georgetown University
Abstract:
The purpose of this paper is to explore how the Internet is altering the landscape of political discourse and advocacy, with particular emphasis on how it is used by those wishing to influence foreign policy. Emphasis is on actions taken by nonstate actors, including both individuals and organizations, but state actions are discussed where they reflect foreign policy decisions triggered by the Internet. The primary sources used in the analysis are news reports of incidents and events. These are augmented with interviews and survey data where available. A more scientific study would be useful.
Available online at: *http://www.nautilus.org/info-policy/workshop/papers/denning.html*

Affecting Trust : Terrorism, Internet and Offensive Information Warfare
Valeri, Lorenzo, Knights, Michael,
Abstract:
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.
Available in the NATO library in: TERRORISM_AND_POLITICAL_VIOLENCE, vol. 12, no. 1, Spring 2000, p. 15-36

Assessing the Risks of Cyberterrorism, Cyber War and Other Cyber Threats
James A Lewis, Center for Strategic and International Studies, Dec 2002
Available online at: *http://www.csis.org/tech/0211_lewis.pdf*

Countering Cyber War.
Shimeall, Timothy
Abstact:

The authors argue that defence planning has to incorporate the virtual world to limit physical damage in the real.
Available in the NATO library at: NATO_REVIEW, vol. 49, Winter 2001 - 2002, p. 16-18.

Cyber-attacks and International Law
Grove, Gregory D.
Abstract:
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.
Available in the NATO library at: SURVIVAL, vol. 42, no. 3, Autumn 2000, p. 89-103

Cyber Attacks During the War on Terrorism: A Predictive Analysis Sept 2002
prepared by the Dartmouth Institute for Security Technology Studies in the US
Available online at: http://www.globaldisaster.org/cyberattacks.pdf

Cyberterrorism - Fact or Fancy?
Mark M. Pollitt , FBI Laboratory
*Abstract***:**
This paper discusses the definition of cyberterrorism, its potential, and suggests an approach to the minimization of its' dangers. The definition of cyberterrorism used in this paper is combines the United States Department of State's definition of terrorism as politically motivated acts of violence against non-combatants with a definition of cyberspace as the computers, networks, programs and data which make up the information infrastructure. The conclusion is that by limiting the physical capabilities of the information infrastructure, we can limit it potential for physical destruction.
Available online at: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html

Cyberterrorism Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives
Dorothy E. Denning, Georgetown University May 23, 2000
Available online at: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

From Car Bombs to Logic Bombs : The Growing Threat from Information Terrorism.
Post, Jerrold M
Abstract:
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.
Availabe at the NATO library at: TERRORISM_AND_POLITICAL_VIOLENCE, vol. 12, no. 2, Summer 2000, p. 97-122.

IDC: Cyberterror and Other Prophecies
Ed Frauenheim, Staff Writer, CNET News.com
December 12, 2002
Available online at: *http://news.com.com/2100-1001-977780.html?tag=fd_top*

The Myth of Cyberterrorism : There are many ways terrorists can kill you--computers aren't one of them.
Joshua Green, The Washington Quartlerly Online
Available online at: *http://www.washingtonmonthly.com/features/2001/0211.green.html*

What is Cyberterrorism ?
Conway, Maura
Abstract:
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.
Available in the NATO library at: CURRENT_HISTORY, vol. 101, no. 659, December 2002, p. 436-442.

Websites:

Center for Strategic and International Studies
Washington DC
http://www.csis.org

Cyber Terrorism Resource Centre
Provides to links to article and commentaries around the world.
http://www.globaldisaster.org/cyberterrorrescen.shtml

Internet / Network Security Resource guide on Cyberterrorism
Listing of websites and articles
http://netsecurity.about.com/cs/cyberterrorism/

IWS United Kingdom Website Listing
Essential documents, articles, news watch, conferences and related links, as they apply to cyberterrorism.
http://www.iwar.org.uk/cyberterror/index.htm

National Cyber Security Alliance
http://www.staysafeonline.info/

Terrorism Questions and Answers : Cyberterrorism
Council on Foreign relations
http://www.terrorismanswers.com/terrorism/cyberterrorism.html

Terrorism questions and answers: Cyberterrorism Europe
Council on Foreign relations
http://www.terrorismanswers.com/coalition/europe.html

vnunet.com
UK: technology news reviews and downloads

http://www.vnunet.com/News/Security

Books:

Combattre le terrorisme international
Benyamin Netanyahou
Available to purchase from fnac.com
Abstract:
Le terrorisme est et sera le fléau des années 2000, comme il fut celui des années 70. Mais il est désormais porteur de nouveaux dangers - menace chimique et bactériologique, puissance logistique et financière, réseaux implantés dans le monde entier - et d'une détermination que rien ne saurait fléchir, comme l'ont prouvé les attentats qui ont récemment endeuillé les Etats-Unis. Aujourd'hui plus que jamais, il importe, pour mieux le combattre, de comprendre les ressorts du terrorisme international. Quels buts - politiques, idéologiques, économiques - poursuivent ses acteurs ? De quels moyens et de quels soutiens disposent-ils ? Doit-on craindre l'avènement d'un " terrorisme nucléaire " ? Depuis trente-cinq ans, Benyamin Netanyahou se consacre à la lutte antiterroriste. Fruit de l'action et de la réflexion, ce livre étudie les origines, les motivations et les développements futurs des groupes terroristes. Il présente en outre dix propositions concrètes pour faire échec à ce fléau et assurer la défense des sociétés occidentales sans restreindre les libertés individuelles. Parmi ces propositions : des sanctions contre les pays fournisseurs d'armes, le durcissement des législations nationales, des programmes de coopération policière, des mesures de rétorsion diplomatiques, économiques et militaires... Initialement publié en 1996, ce livre prophétique - il évoquait, cinq ans avant, l'hypothèse de la destruction du World Trade Center - est précédé d'un nouvel avant-propos de l'auteur.

Computer Network Attack and International Law
Michael N. Schmitt & Brian T. O'Donnell, editors 2002
Available via ILL from Bibliotheques de 'Universite Libre du Bruxelles

Cybercrime, Cyberterrorism, Cyberwarfare : Averting an Electronic Waterloo.
Center for Strategic and International Studies
Available via ILL from the Bristish Library

Forces spéciales, Guerre contre le terrorisme
Eric Micheletti
Available: 15 avril 2003
Available to purchase from fnac.com

The Information Revolution and National Security - Carlisle Barracks, PA : US Army War College. 141 p. ISBN: 1584870311 US Army War College. Strategic Studies Institute
Abstract:
'The current era has seen more rapid and extensive change than any time in human history. The profusion of information and the explosion of information technology is the driver, reshaping all aspects of social, political, cultural, and economic life. The effects of the information revolution are particularly profound in the realm of national security strategy. They are creating new opportunities for those who master them. The US military, for instance, is exploring ways to seize information superiority during conflicts and thus gain decisive advantages over its opponents. But the information revolution also creates new security threats and vulnerabilities. No nation has made more effective use of the information revolution than the United States, but none is more dependent on information technology. To protect American security, then, military leaders and defense policymakers must understand the information revolution.'

Available at the NATO library: 355.4 /1274 ID number: 80016781

Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age
by Winn Schwartau
An expert on electronic privacy shows how "information warriors" are able to gain access to and use computerized data on ordinary individuals, and the threat such use poses to citizens and to national security.
Available from Amazon.com

Information Warfare : How to Survive Cyber Attacks.
Michael Erbschloe New York. London. Osborne/McGraw-Hill. c2001
Abstract:
Another release in our popular "Computer World: Books for IT Leaders" series, Information Warfare explains the methodologies behind hacks and cyber attacks and provides defensive strategies and counter measures designed to help companies survive infrastructure attacks, military conflicts, competitive intelligence gathering, economic warfare, and corporate espionage. The authors are renowned industry experts--Michael Erbschloe has connections with the government and is known for his analysis of The Love Bug
Available via ILL from the British Library

Networks and Netwars : The Future of Terror, Crime, and Militancy - Santa Monica, CA : Rand Corporation. 375 p. ISBN: 0833030302 Year: 2001
Abstract:
'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.'
Available at the NATO library: 355.4 /1348 ID number: 80018284

Protection juridique du cyber consommateur
T. Verbiest
Available to purchase from fnac.com

Technology and Terrorism : The New Threat for the Millennium - Leamington Spa, UK : RISCT. 24 p. Author(s): Bowers, Stephen R., Keys, Kimberly R.
Abstract:
'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.' Year 1998
Available at NATO Library: 323/629 ID number: 80014853

Le terrorisme non conventionnel
O. Lepick, J.F. Daguzan
Available: 15 mars 2003.
Available to purchase from fnac.com

Transnational Threats : Blending Law Enforcement and Military Strategies - Carlisle Barracks, PA : US Army War College. 256 p Year: 2000 ISBN: 1584870370
Abstract:
'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.'
Available at the NATO library: 323/676 ID number: 80017080

The Transnational Dimension of Cyber Crime Terrorism.
editors, Abraham D. Sofaer, Seymour E. Goodman. contributing authors: Mariano-Florentino Cuellar ... [et al.] Stanford, CA. Hoover Institution Press. 2001
Based on a conference on international cooperation to combat cyber crime and terrorism, held at the Hoover Institution on December 6 and 7, 1999
Available via ILL from the Bristish Library

Terrorisme et contre-terrorisme
B. Courmont
Available to purchase from fnac.com