Defense & Security Analysis Vol. 19, No. 2, pp. 165–175, 2003

Carfax Publishing
Taylor & Francis Group

Ethics and International Security in the Information Age

Joelien Pretorius

Centre for International Political Studies, University of Pretoria, 0002 South Africa

According to Moore's Law, every 18 months technology is developed reducing electronic systems to half their previous size.[1] The resultant impact upon the field of information and communication has been revolutionary and can be framed in terms of three orders of manifestation. The first order manifestation of the information revolution is technological and refers to the unprecedently cheap, fast and user-friendly information devices that have been developed in the past two to three decades. Digitization, miniaturization and conversion of different media into each other have been the impetus for a worldwide communications infrastructure – the apex of which is the Internet. The first order (or technological) implications of the information revolution have, in the second order, impacted on social, political and economic activities allowing for the almost instant mobility of capital, the proliferation of multinational corporations, the global reach of news media coverage, and cross-border mobilization of individuals and interest groups. The behavioral implications of the information revolution, in the third order, raise questions of a structural nature about the validity of the nation-state, the expression of identity and the organization of the international community. This article aims to tease out the ethical implications of the technological, behavioral and structural dimensions of the information revolution and in turn international security in two ways. First, the impact of information technology (IT) on contemporary ethical issues in the pursuit of international security, for example weapons of mass destruction (WMDs) and redistributive justice and human rights, are explored. Second, IT also introduces a whole new set of ethical questions to international security issues. These questions are most often related to the causes and conduct of war, personal privacy in opposition to state security, and information inequality.

ISSN 1475-1798 print; 1475-1801 online/03/020165-11 © 2003 Taylor & Francis Ltd
DOI: 10.1080/1475179032000083370

IT AND CONTEMPORARY ETHICAL ISSUES IN INTERNATIONAL SECURITY

In many respects, IT has contributed to international security by impacting positively on the areas of diplomacy, arms control and the mobilization of international public opinion. Diplomacy has changed in the information age from "elite groups within national governments communicating about international problems only with each other, and largely behind closed doors"[2] to include a wider audience in two ways.[3]

Public diplomacy

It is increasingly a matter of political necessity for governments to communicate and justify their foreign policy intentions both domestically and internationally. Democracies, in particular, can no longer act without getting the support of foreign publics. If they alienate a foreign public, the government of that state may be less inclined to support the policy in full. This is due to the so-called CNN effect, that is probably better termed the CNN *et al.* effect.[4] This effect refers to the reach and impact that news channels, such as those of CNN and the British Broadcasting Corporation (BBC) have on global audiences when they feature a news story. There have been speculations that the US refusal to ratify the Kyoto Protocol and the subsequent outcry in the international media and global public sphere resulted in the US being voted out of two key United Nations (UN) organs, the UN Commission on Human Rights and the UN International Drug Control Board, in May 2001.

Although this kind of digital global public may place normative constraints on foreign policy, it should not be taken for granted that this will actually enhance ethics in foreign policy. It may have the adverse effect of encouraging states to act unilaterally instead of seeking compromise and consent with other nations. Moreover, in undemocratic states, the role which public diplomacy plays may be reduced. In the aftermath of the September 11, 2001 attacks on the United States, the Bush government used economic diplomacy as well as coercion – threatening that those states, which do not support the US in their retaliatory efforts will be considered against the US in the war against terrorism – to round up allies. In Pakistan, the persistence of grassroots anti-American protests has not detracted the Musharaff government from supporting the US.

Virtual diplomacy

Virtual diplomacy may describe the way in which IT has broadened and deepened the opportunities for diplomatic efforts through a diverse variety of networked channels. The Internet has been instrumental in allowing expert groups to act as intermediaries, advocates and advisers in international conflicts, and arbitration and conflict resolution networks have sprung up on the Internet. They are run by various institutes and research centers that identify parties in a conflict and try to engage them in dialogue. The University of California's Institute on Global Conflict and Co-operation (IGCC) embarked on a project called "Wired for Peace". The project aims to link social scientists and policy-makers with science and technology experts to develop Internet applications for multilateral co-operation in the Middle East and Northern Asia. Track-two communications and co-operation between key players through access to multilingual document libraries, workgroup schedules and tools for collaborative document writing and data analysis were designed to strengthen peace processes and are also referred to as virtual track-two diplomacy.[5] The other side to virtual track-two diplomacy involves people-to-people interaction where citizens learn directly from counterparts in other countries. The personal nature of virtual diplomacy means that it is a potentially powerful means of mobilizing public opinion and influencing government policy. Virtual diplomacy contributes to raising the ethical stakes in foreign policy by offering direct channels of interaction between those involved in different ethical and moral issues. It provides a way to limit what would otherwise not be considered ethical foreign policy.

The information revolution has made it easier to monitor the adherence of states to internationally agreed codes of conduct (conventions, treaties and protocols). This is especially true in the realm of arms control where the impact of IT on the nuclear weapons issue serves as an example. The network of portable, low-cost seismometers run by hundreds of digital stations around the world, monitors seismological events, including nuclear tests. This has not prevented states from testing nuclear weapons (as seen by the Indian and Pakistani tests in 1998), but it does mean that states cannot test covertly.[6] IT may allow for anonymous information gathering regarding chemical, biological or nuclear weapons.[7]

In the realm of redistributive justice and human rights, it is the second order manifestations of the information revolution, such as the proliferation of transnational corporations and global movements promoting issues of moral concern, that impact on ethics in foreign policy. On the one hand, IT has played a pivotal role in the ability of corporations to "slice up the value chain", and to allocate different production phases to different locations. Transnational corporations have frequently sought locations where it is cheapest and easiest to complete their different stages of manufacturing. This has sometimes resulted in the exploitation of workers in countries where labor and environmental laws are less stringent, most often in developing countries. This has led to considerable opposition to global financial institutions, such as the World Trade Organization (WTO), the International Monetary Fund (IMF) and the World Bank, and governments seen to be promoting globalization. Groups opposing globalization have utilized the Internet to express their views, mobilize support, organize activities and inform the public, in turn putting pressure on governments, international organizations and transnational corporation to account for their policies. In a similar fashion, the Internet was instrumental in banning blood diamonds and anti-personnel landmines and putting the cancellation of foreign debt on the international agenda.

IT AND NEW ETHICAL ISSUES IN THE PURSUIT OF INTERNATIONAL SECURITY

The information revolution has raised new ethical questions in several areas of international security, most notably those of warfare, propaganda, and surveillance and information inequality.

The reconceptualization of warfare in the information era portrays a rationalist inclination, focused largely on its impact on the physical security of the state in the event of war. This approach was made fashionable by Heidi and Alvin Toffler[8] in *War and Antiwar*, which employs the term "information warfare". It superimposes the use of information technologies for conflict and the conduct of military operations on the emerging geostrategic environment of states. Information warfare, on the one hand, involves the military application of IT to achieve strategic objectives and, on the other, the targeting of information infrastructure to debilitate and/or defeat an enemy. In terms of the former, information-rich states will pursue information dominance as the US military refers to its information advantage over its enemies as a result of information disparity.[9] This has led to considerations of a revolution in military affairs (RMA),[10] driven by the information revolution and encompassing "deep-strike dominated, stealthy air operations; land and space-based defense of the sea and submersible power projection; space warfare; and independent and integrated information warfare".[11] The Gulf War was seen as the first, albeit incomplete, example of the RMA and US information dominance.

In terms of targeting civilian and military information infrastructure to debilitate an enemy, information-rich states have increasingly become concerned about their dependence on IT in civil and military affairs, making them more vulnerable than states that are less penetrated by IT.[12] National security analysts in information-rich countries have subsequently been concerned about information asymmetry or the so-called David effect, which refers to the potential of IT to allow small states to win a conventional war against a major power. This might be done by acquiring the right technology and building up a small army of so-called cyber warriors (IT specialists and programmers that can hack into another state's most important computers). Victory might be made affordable by entering an enemy's computer-controlled infrastructure and disrupting critical services, creating false information, and launching malicious logic-based weapons against their information systems[13] than "by fighting them on the beaches".

Foreign policy-makers deal with the political dimension of security and need therefore to be aware of the ethical questions that arise by reconceptualizing warfare in this way. It is the political environment that determines the climate between states, in turn influencing the ethical thresholds that will limit and control how information warfare is waged. These ethical questions may include the following.

The unpredictability of an adversary's response to high-tech warfare

At first the idea of precision-guided munitions (PGM)[14] was hailed as the key to more humane warfare. It provided means to lessen collateral damage and reduce the number of troops in the field.[15] But, when states do not have the capacity to respond in kind to these high-tech attacks they may resort to whatever means they have. Russian military theorists have, for example, argued that the use of PGM against them must be seen as the beginning of a nuclear war, for they have no conventional way of responding to such an attack, but to go nuclear. In practice, responses to counter PGM attacks have included collocating targets with non-combatants. During the bombing of Yugoslavia by the NATO forces civilians gathered on Belgrade's bridges, while Saddam Hussein was reported to have filled his presidential palace with civilians when Western military action seemed forthcoming in 1997.[16]

The difficulty of discriminating between civilian and military targets

The principle of discrimination is recognized by the laws of just war and *jus in bello*. In an age when it is increasingly difficult to distinguish between military and civilian systems, upholding this principle has become an ethical question.[17] More than 90 percent of the US Armed forces' command and control information flows through commercial channels, which, with other dual-use systems, may make them legally and ethically justifiable targets.[18] But, targeting these systems will have implications for essential civilian services, such as power supplies and traffic control.[19] Computer network attacks (CNAs), through a non-discriminatory virus, may have unintended consequences, even affecting those not remotely involved in the conflict. Once a virus is deployed it might readily spread through the Internet to computers around the world.[20]

Lowering the threshold of conflict

Dunlap also voices concern over the possibility that new technologies may lead to a lowering of the threshold for conflict.[21] PGM attacks, resulting in collateral damage, and non-attributable deaths may therefore increasingly be used in pre-emptive strikes and "diplomatic" messaging, as was the case in the post-Gulf War uses of PGM against Iraq. However, the response of those subject to CNAs is uncertain and may, potentially, lead to lethal retaliation.[22]

Distinguishing between prudent preparation and hostile action

Hardware modification such as "chipping"[23] (adding a microchip that will delete or alter key functions of a computer) as a strategy of information warfare might be done during peacetime and activated in wartime. The question is whether such a strategy constitutes prudent preparation or a hostile action? Is chipping a hostile action if it is only activated during wartime, and does such an act not constitute a legitimate act of belligerence allowed by a state of armed conflict?

Dealing with conflict between states and non-state actors

The Internet has permitted like-minded individuals to align themselves and in some cases to create virtual political entities, such as the Kurdish parliament. Yet, the institutional norms in the international system are still set within the frame of a state system where the actors who negotiate the deals are linked to geography. The US bombing of Afghanistan in the war against terrorism signifies the lag between the reality of borderless alignment and a mind-frame of geographically bounded entities. The way in which states interact with virtual political entities becomes an ethical issue when civilians in Afghanistan have to pay the price for a global terrorist network of which the mastermind happens to be protected by an illegitimate government.

When virtual political entities are indiscriminately regarded as sources of state ungovernability and political fragmentation, they may undermine human rights, democracy and the right of groups to associate and express themselves freely.

Censorship and propaganda in the era of global communications

The ideal of information dominance in the battlefield brings about another ethical question. The data available from third-party sources, including global media, commercial satellites and the Internet may encourage states to employ unethical measures against international sources of information, either through censorship and broadcast limitations or by making use of propaganda. Although propaganda has always been a dimension of foreign policy, especially in times of war, the increased capacity for spreading disinformation warrants a re-examination. Altering the images of hostile leaders and projecting them back to their people may dramatically influence democratic processes. Dunlap[24] argues that governments may want to develop policies that restrain "information warriors" from damaging the democratic process in enemy states because democracy has an intrinsic human value that may actually deter governments from war.

Manufacturing consent

The question is whether the global mass media (CNN *et al.*) is not already guilty of "manufacturing consent" as Noam Chomsky would refer to implanting the doctrine of the state line in disregard to surrounding facts or evidence to the contrary.[25] A symbiosis between government and media coverage of international affairs may be created by governments, restricting and/or manipulating media access to information and coverage.[26] This was especially the case during the Gulf War, which is often referred to as the first state-managed television war in history: 80 percent of the US public getting their information from television supported the war. The US government seems intent on following the same strategy in the war on terrorism after the September 11 attacks.[27]

Biased reporting on international issues (hegemonic internationalism)

The global media may contribute to the constitution of an international public sphere where international society can participate in a common conversation or "global dialogue", transcending international enmities. This was the case during the US/Soviet summits in Italy near the end of the Cold War. The meetings between Reagan and Gorbachev were usually sketched as integrating events in which the whole of mankind had a stake.[28] However, the international public sphere created by the global media is often subject to hegemonic internationalism; that is, "the belief that the integration of the world is taking place but on asymmetrical, unequal terms, and that this is the only possible and desirable way for such an integration to take place".[29] Coverage devoted to different areas of the world and their responses to issues are skewed. Moreover, when these parts of the world are reported on, it is done through culturally confined lenses. Kavoori writes that the narratives used by American and British journalists serve the foreign policy interests of their governments and manufacture consent in public opinion.[30] The narratives often dichotomize, dramatize and distort the issue at stake, resulting in a perception of "we" (the good, lucky or prosperous ones) versus "them" (the bad, unhappy or destitute ones). Coverage surrounding the response of Palestinians to the September 11 attacks seems to be an egregious example. Footage was shown of

Palestinians celebrating in the streets after news of the attack, but no coverage of Palestinians reportedly carrying candles in front of the US Embassy in Jerusalem or the minute of silence observed by Palestinian children were shown.

Biased reporting may extend beyond nationalism to the protection of business interests. It has been alleged that the soft approach towards China taken by the newspaper, *The Times*, and publishing house, HarperCollins, is a factor of their owner, Rupert Murdoch's business interests in China and that this also explains his access to satellite systems covering China, denied to the BBC.[31]

Bringing "Big Brother" to life through global surveillance and espionage systems

The debate on the ethics of surveillance in the information era was tabled when the Science and Technology Options Assessment Panel of the European Parliament (STOA) accepted the IC2000 report on communication interception and ECHELON as a working document at their meeting in Strasbourg on May 6, 1999. This report, which was first presented to the European Parliament in 1998, exposed the existence of a global surveillance system, referred to as ECHELON, comprising US (National Security Agency/CIA), UK (GCHQ), Canadian, Australian and New Zealand intelligence activities. This network, created during the Cold War, has five centers in each of the aforementioned countries, which provide intelligence on keywords, phrases and people. Analysts believe that e-mail, and to a lesser extent telephone and fax communication within the scope of this system, could be routinely intercepted and transferred to the relevant center. Criteria determining who is not a target of surveillance are unclear. As a result of this type of indiscriminate surveillance the legitimacy of the information gathered by the ECHELON system has come under scrutiny. There have even been reports that US and UK corporations have benefited from information gathered by ECHELON at the cost of their European and Japanese counterparts, but these claims could not be verified. Although ethical considerations of surveillance and espionage are not new, the extent to which governments can gather information may necessitate ethical guidelines regarding legitimate targets of surveillance and the use of information gathered.

The September 11 attacks have also reignited the debate about encryption, which restricts the ability of third parties, including law enforcement and intelligence agencies, to read intercepted digital messages by "scrambling" data and then restoring it to its original form by using a decryption "key".[32] It is reported that the terrorists coordinated the attacks over the Internet using encryption and/or hiding messages in picture files on pornography web sites.[33] Although this has not been confirmed, the US Justice Department has called for laws that would enable investigators to circumvent encryption. These laws would include legally mandated key recovery for encryption software and export restriction on encryption. However, unless there is a global prohibition on the use of strong encryption without a back door for government surveillance, the proposed laws will have little effect as encryption software can be downloaded for free from the Internet. The argument against restrictions on encryption is firstly based on the protection of personal privacy – a fundamental right in most democratic constitutions. Second, software companies argue that overly strict encryption regulations inhibit the technology market, reduce international competitiveness and leave customers with little confidence in on-line commerce. Third, a security argument is made that strong encryption protects critical infrastructure, because it is used in burglar alarms, cash machines, ticket systems and postal meters. Widespread insertion of key recovery systems, thus increasing the number of people with authorized access to critical infrastructure and business data, will ease attack, whether through technical means or by exploitation of mistake or corruption.[34]

Addressing information poverty

Information poverty and the "digital divide" add to the complexity of ethical foreign policy in several respects. First, if access to the Internet, as the main tool for creating a global civil society, is skewed, the result may well be a biased civil society that promotes the ethics of information-rich societies. Second, information-poor countries may be less penetrated by information networks and therefore an attack on their strategic information infrastructure may have a lesser effect on their critical services than in an information-rich country. As the threat of information warfare, terrorism and crime increase, a situation may arise whereby information-rich countries will have an incentive to prevent the spread of certain information technologies, in turn creating a club of "responsible information haves", resembling that of the nuclear weapons states.

Although many ethical issues identified are covered in existing treaties, conventions and international agreements, there is a need to explicitly codify norms governing the new ethical questions arising from the information revolution. There has been a tentative movement in the realm of international co-operation to counter cyber crime and terrorism. The Council of Europe has, for example, drafted a Convention on Cyber Crime, and more recently members of government, industry, non-governmental organization and academia have congregated at Stanford University to discuss international abuse of cyber systems and build a co-operative framework. A proposal for an International Convention on Cyber Crime and Terrorism has subsequently been drafted to incorporate the ideas expressed at the Conference.[35] An international convention of this kind may be the precursor to an information security regime. The implications of such a regime for foreign policy-makers are far-reaching. It may incorporate treaties on information warfare that mirror those on weapons of mass destruction, as well as creating cyber confidence-building mechanisms and perhaps, even, the creation of a cyber peacekeeping capacity.

In addition to an information security regime, information-poor states may wish to revisit the idea of a New World Information and Communication Order (NWICO), which was promulgated in the United Nations Education and Science Organization (UNESCO) in the 1980s to address information poverty.

CONCLUSION

Unlike the introduction of nuclear technology into the ethical agenda of international security on August 6, 1945, the awareness of the ethical implications of information technology has evolved in a much more gradual and haphazard fashion. For normative theorists this should be an issue of concern for it leaves open an opportunity for rationalists to develop and entrench their own vocabulary for information technology and foreign policy in rationalist terms. These considerations not only include an acceptance of the state system and international anarchy as the basic premises of international relations, but also involve doing away with positions and "imprecise" statements that cannot be tested through developing theory and empirical study. The new (and in many ways uncertain) circumstances brought about by the information era, probes a more radical or reflectivist theoretical approach. IT is more than just a way to develop "value-free" instruments that can be used by states in their pursuit of foreign policy objectives. IT should be viewed as a constitutive of reality with embedded values that should be exposed, allowing for ethical implications of foreign policy to be debated internationally.

Although the September 11 attacks have served to highlight many of the ethical implications of the information revolution for international security, the emphasis in discourse surrounding the attacks has largely been placed on the purely technological manifestations (first order) and their possible contribution to the successful execution of the attacks. The emphasis is misplaced for two reasons. First, it is unclear to what extent the plans for the attacks were really that high-tech. Some have argued it is precisely the low-tech nature of the operation that warranted its success and blame the US intelligence agencies' focus on communications intelligence as opposed to human intelligence for their ignorance of the planned attacks.[36] Second, the second and third order manifestations of the information revolution may be a more appropriate focus for the ethics and IT debate. Globalization of financial markets has made it increasingly difficult to track and scrutinize the financial assets and money transferring networks that sustain terrorist activities. The adverse affects of globalization on poor states, the dominance of Western culture through biased global media coverage, and the perceived arrogance in the foreign policies of economic and technological superior states may be greater causes of ethical concern after the September 11 attacks.

NOTES

1. K. Kruszelnicki, "Less is Moore", *Great moments in Science*, 2000. Http://www.abc.net.au/science/k2/moments/s137447.htm
2. W. R. Roberts, "Diplomacy in the Information Age", *World Today,* 47(4), July 1991, pp. 112–116.
3. M. Tehranian, *Global Communication and World Politics: Domination, Development, and Discourse*, Boulder: Lynne Rienner, 1999, pp. 63–68.
4. M. Libicki, "Information War, Information Peace", *Journal of Internal Affairs*, 51(2), 1998, pp. 411–428.
5. C. Gormley, "Getting Wired for Peace", *The World Today*, 55(3), March 1999, pp. 18, 19.
6. Libicki, "Information War, Information Peace", *Journal of Internal Affairs*, 51(2), 1998, pp. 411–428.
7. B. Larkin, "Can Computers and Communication Enhance Global Security?", paper presented to the 20th ISODARCO Summer School, *Computers, Networks and the Prospects for European and World Security*, August 7–17, Rovereto, Italy, 1999, p. 4
8. A. Toffler and H. Toffler, *War and Anti-war: Survival at the Dawn of the Twenty-First Century*, London: Warner Books, 1994.
9. D. J. Rothkopf, "Cyberpolitik: The Changing Nature of Power in the Information Age", *Journal of International Affairs*, 51(2), Spring 1998, pp. 325–59.

10. In historical context the term "revolution in military affairs" refers to the changes that militaries undergo as a result of technological change (often associated with conceptual changes about the role of the military and the conduct of war). The term became fashionable after the Gulf War with the employment of PGM that changed the very way the war was fought.
11. M. Vikers, "The Revolution in Military Affairs and Military Capabilities", in R. L. Pfaltzgraff and R. H. Schultz, *War in the Information Age: New Challenges for US Security Policy*, Washington: Brassey's, 1997, p. 32.
12. R. L. Pfaltzgraff and R. H. Schultz, "Future Actors in a Changing Security Environment", in R. L. Pfaltzgraff and R. H. Schultz (eds), *War in the Information Age: New Challenges for US Security Policy*, Washington: Brassey's, 1997, p. 13.
13. D. J. Rothkopf, "Cyberpolitik: The Changing Nature of Power in the Information Age", *Journal of International Affairs*, 51(2), Spring 1998, pp. 325–359.
14. PGM are associated with information warfare inasmuch as these (smart) weapons make use of microchip technologies and their use is seen as the beginning of the revolution in military affairs associated with information technology.
15. W. Bayles, "The Ethics of Computer Network Attacks", *Parameters*, Spring 2001, pp. 44–58.
16. C. Dunlap, "Technology: Recomplicating Moral Life for the Nation's Defenders", *Parameters*, Autumn 1999, pp. 24–53.
17. W. Bayles, "The Ethics of Computer Network Attacks", *Parameters*, Spring 2001, pp. 44–58.
18. D. Kuehl, "The Ethics of Information Warfare and Statecraft", *Infowar.com*, 2000, http://www.infowar.com/mil_c4i/mil_c4ij.htm-ssi
19. C. Dunlap, *op. cit.*, pp. 24–53.
20. S. Nitzberg, *Conflict and the Computer: Information Warfare and Related Ethical Issue*, 1998, http://www.telos.com/corpinfo/feature/pdf/conflict.pdf
21. C. Dunlap, *op. cit.*, pp. 24–53.
22. D. Kuehl, *op. cit.*
23. D. Kuehl, *ibid.*
24. C. Dunlap, *op. cit.*, pp. 24–53.
25. T. Bhattacharya, *A Talk on Chomsky's Manufacturing Consent*, 1995, http://ucl.ac.uk/~uclytbh/consent.htm
26. M. Tehranian, *Global Communication and World Politics: Domination, Development, and Discourse*, Boulder: Lynne Rienner, 1999, p. 64.
27. E. Bumiller, "New Slogan in Washington: Watch What You Say", *New York Times*, October 7, 2001, http://www.nytimes.com/2001/10/07/national/07PRES.html
28. D. Hallin and P. Macini, "Summits and the Constitution of an International Public Sphere: The Reagan-Gorbachev Meetings as Televised Media Events", *Communication*, Vol. 12. 1991, pp. 249–265.
29. F. Halliday, "Three Concepts of Internationalism", *International Affairs*, 64(2), 1988, pp. 187–198.
30. A. P. Kavoori, "Between Narrative and Deception: Toward a Cultural/Contextualist Model of Foreign Policy Reporting and Public Opinion Formation", *Journal of International Communication*, 4(1), 1997, p. 104.
31. K. Haggart, *Further Controversy Erupts Over Murdoch,* China Freedom Forum.org. http://www.freedomforum.org/templates/document.asp?documentID=5045
32. D. Froomkin, *Deciphering Encryption*, Washingtonpost.com. http://www.washingtonpost.com/wp-srv/politics/special/encryption/encryption.htm. Updated May 8, 1998.
33. J. Kelley, "Terror Groups Hide Behind Web Encryption", *USA Today*, http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm#mor
34. H. Abelson *et al.*, *The Risks of Key Recovery, Key Escrow and Trusted Third Part Encryption*, report by an *ad hoc* group of cryptographers and computer scientists, www.cdt.org/crypto/risks98/

35. A. Sofaer *et al.*, *A Proposal for an International Convention on Cyber Cime and Terrorism*, Augustus 2000, http://www.iwar.org.uk/law/r . . . ime/stanford/cisac-draft.htm
36. Mark Ward, "Tackling Terror with Technology", BBC News Online, September 21, 2001, http://news.bbc.co.uk/hi/english/sci/tech/newsid_1555000/1555981.stm