Chapter 9

The G8 and the Governance of Cyberspace

Jeffrey A. Hart

The representatives of the countries that comprise the G7/8 began to address the problems of co-ordinating policies regarding the governance of cyberspace in the early 1990s. Initially, they deal with governance issues including, among others, the establishment of norms, principles, and rules regarding the interconnection of computer networks via networks of networks such as the internet, rights of access to those networks, pricing of access, monitoring of network-mediated economic transactions, intellectual property protection, taxation of goods and services delivered though the networks, privacy, security, and a variety of other matters thought to affect the confidence of users. Toward the end of the decade, the G8 turned to a new issue: reversing the tendencies toward an increasing 'global digital divide' between rich and poor countries. After 11 September 2001, the G8 turned its attention to a variety of cyberspace security issues and began to link its digital divide discussions to broader questions related to North-South relations, focussing particularly on the Middle East and the rest of the Islamic world.

One of the key questions addressed here is why the G8 turned from the previous set of cyberspace governance issues in 1999 to a consideration of how to bridge the digital divide. This chapter posits that the main reason was the G8's need to respond to the criticisms by antiglobalisation forces that G8 governance was undemocratic and therefore contributed to increased global inequality. For this reason, one important way to evaluate the success of the G8 in this area was in terms of its ability to provide a counterargument to the claims of the antiglobalisation movement. More important, however, was the attempt by the G8 to transcend its inherently intergovernmental character by including representatives from civil society in its deliberations on the global digital divide. The Digital Opportunity Task Force (Dot Force) invented a method called the 'multistakeholder approach' to do this. Many of the participants in the Dot Force considered this invention to be a success, but only time will tell whether the approach will spread to other issues under G8 purview.

The shift of attention after 11 September toward security concerns temporarily diverted the G8's attention away from North-South issues and toward preventing cyber-attacks and cyber-terrorism mainly in the North. Although these may at first sight appear to be traditional national security concerns, the heavy reliance on the private

sector to build and maintain computer and telecommunications networks made the multistakeholder approach innovated by the Dot Force of continuing relevance to G8 deliberations. In addition, the problem of winning the hearts and minds of those who could potentially be recruited to terrorist causes would require an eventual return to issues connected with North-South inequalities such as the global digital divide.

Historical Context

Although originating in the late 1960s in research begun under the auspices of the United States Department of Defense Advanced Research Projects Agency (ARPA), the internet emerged in the 1990s as the most important network of networks with the capability, in principle, to interconnect every computer (large or small) on the planet. While the ARPANET was built in the 1970s to interconnect military contractors with one another, it was succeeded first by the NSFNET (National Science Foundation Network), which expanded interconnection to university scientists and engineers, and then by the internet. Commercial interconnection to the internet began in the late 1980s, and soon many businesses had shifted at least some of their activities to cyberspace (Hart, Bar, and Reed 1992).

By the early 1990s, the U.S. government began to ask the rest of the world to adopt policies that it believed would be conducive to the spread of internet-based commercial activity. This was the Global Information Infrastructure (GII) initiative of the Clinton administration.

One particularly important aspect of the GII initiative was the push for policies of minimal restrictions on e-commerce in order to encourage the shift of economic transactions to the internet. According to *The Framework for Global Electronic Commerce*, there was a danger of killing off the goose that lays the golden eggs:

> Commerce on the Internet could total tens of billions of dollars by the turn of the century. For this potential to be realized fully, governments must adopt a non-regulatory, market-oriented approach to electronic commerce, one that facilitates the emergence of a transparent and predictable legal environment to support global business and commerce. Official decision makers must respect the unique nature of the medium and recognize that widespread competition and increased consumer choice should be the defining features of the new digital marketplace (White House 1997).[1]

The Clinton administration called on the World Trade Organization (WTO) to declare the internet a tax-free environment and to request the development of a uniform commercial code for electronic commerce. The U.S. asked that there be a WTO effort to make national intellectual property regimes more consistent and enforceable. A series of reports was issued to provide background information for these and other related policy proposals over the next three years (Smith et al. 2001, 12). The U.S.

government was largely successful in these policy initiatives, although not without generating considerable controversy.

The Clinton administration also called for a meeting of the information ministers of the G8 in 1995 to be held on 25–26 February in Brussels. The main topic of discussion was the means by which to 'encourage and promote the innovation and development of new technologies, including, in particular, the implementation of open, competitive, and world-wide information infrastructures' (Information Society Website 1995). The conference concluded with the identification of a set of pilot projects that would benefit from international co-operation. These projects were adopted formally and funded by the G8 at the following summit.

At around the same time, in 1995, a joint symposium of the Asia-Pacific Economic Cooperation (APEC) countries and the Organisation for Economic Co-operation and Development (OECD) met in Vancouver to address 'Building the Foundation for the 21st Century'. The APEC-OECD symposium laid the framework for a market-led policy for infrastructure and service development. The OECD followed up in Turku, Finland, in 1997 with a joint government and business conference on the theme of 'Dismantling the Barriers to Global Electronic Commerce'. In 1998, the OECD held a ministerial conference in Ottawa on 'A Borderless World: Realizing the Potential of Electronic Commerce' (OECD 1998). It was at this conference that the members of the OECD agreed to the Ottawa Taxation Framework Conditions (see below). APEC also held follow-up meetings that focussed on using the internet and information technologies to solve problems of economic development. These meetings probably influenced later discussions on bridging the digital divide among the G8 (Beaird 2003).

The World Bank formed the Global Information Infrastructure Commission (GIIC) in February 1995. Its first full meeting took place in Washington in July 1995, and it has met annually since then. The GIIC was designed to facilitate co-operation between governments and the private sector in order 'to foster private sector leadership and private-public sector cooperation in the development of information networks and services to advance global economic growth, education and quality of life' (GIIC 1995).

Internet Governance Issues at the Organisation for Economic Co-operation and Development

The OECD began to take up issues connected with the internet and electronic commerce in the late 1990s. One major effort was connected with the Ottawa Taxation Framework Conditions of 1998. That agreement set out a variety of principles to be followed by OECD governments regarding the taxation of the emerging sector. One principle stated that taxation should be neutral with respect to conventional and electronic forms of commerce. The other general principles to be followed involved neutrality, efficiency, simplicity, effectiveness, fairness, and flexibility. Follow-up work on the framework was delegated to the OECD's Committee on Fiscal Affairs (OECD 2003a, 11–12).

Within the OECD, there has been substantial debate about direct taxes, such as sales taxes. A large issue of contention is determining taxation rights. Under the OECD Model Tax Convention, such taxes require the concept of a 'permanent establishment', a 'fixed place of business through which the business of an enterprise is wholly or partly carried on' (OECD 2000). Preliminary discussions determined that a website is not such a permanent establishment, nor is the internet service provider that hosts the website. Discussion of this issue continues in the OECD.

At the 1998 Ottawa meeting, the OECD ministers reaffirmed 'their commitment to the protection of privacy on global networks in order to ensure the respect of important rights, build confidence in global networks, and to prevent unnecessary restrictions on transborder flows of personal data' (OECD 2003b, 12). They agreed to take the necessary steps to extend the existing OECD Privacy Guidelines (published in 1980) to global networks. Progress in achieving this goal was discussed at the Paris Forum in 1999 and the Emerging Market Economies Forum in Dubai in 2001.

The OECD's Committee for Information, Computer, and Communications Policy and that Committee's Working Party on Information Security and Privacy were given the task of formulating an action plan for online privacy protection. They focussed on the following subtasks:

- Encouraging the adoption of privacy policies.
- Encouraging online notification of privacy policies to users.
- Ensuring that enforcement and redress measures are available in cases of non-compliance.
- Promoting user education and awareness about online privacy and the means at their disposal for protecting privacy.
- Encouraging the use of privacy-enhancing technologies.
- Encouraging the use and development of contractual solutions for online transborder data flows (OECD 2003b, 13).

Part of what was going on here was an adjustment of earlier policies regarding trans-border flows of personal data. In the 1980s and 1990s, the European governments had moved in the direction of stronger guarantees for privacy of online personal data than existed in the United States. Accordingly, they placed rather strict limits on transborder flows of personal data. However, the rapid rise of internet data traffic and e-commerce resulted in a reconsideration of those earlier decisions. European authorities did not want the EU to be excluded from the benefits of e-commerce because of overly restrictive privacy guarantees. In addition, the U.S. government and many U.S.-based multinational corporations (MNCs) strongly urged a relaxation in European privacy guarantees in order to maximise the potential benefits to all of moving to web-based commerce. Therefore, in pursuit of greater international harmonisation of privacy policies within the OECD, there was considerable support for greater transparency of national privacy rules and practices.

It quickly became apparent to participants in these discussions that governments were dependent on private firms to implement and enforce privacy guarantees, since most OECD countries had privatised to some extent the ownership of data conduits and personal data storage systems. Accordingly, private firms were invited to participate in OECD policy discussions. As in other areas of global governance, other private sector groups and organisations asserted their rights to participate in discussions of privacy. For example, Marc Rotenberg (2003) of the Electronic Privacy Information Center (EPIC) presented a plan for integrating civil society organisations into OECD discussions of online privacy matters at the Global Forum on Information Systems and Network Security held in Oslo, Norway, in October 2003. Rotenberg stressed the importance of going beyond government and private business participation in such discussions because of the need to foster consumer trust in global networks in order to realise their potential benefits.

A lot of the activity in this area and in the related areas of authentication (electronic signatures) and cyber-security has related to raising consciousness. A survey of EU businesses done for the European Commission, for example, revealed that 75 percent of companies had no cyber-security strategy whatsoever. Spending in this area was very low and most companies had understaffed information technology security offices (Skantze 2003). Similarly, many governments were struggling to deal effectively with problems of consumer confidence posed by viruses, worms, and spam, often with inadequate resources. It is not surprising, therefore, that international discussions such as those in the OECD would focus on information sharing and the pooling of costs in dealing with these increasingly global problems.

The Global Digital Divide

In 2000, the U.S. Commerce Department's National Telecommunication and Information Administration ([NTIA] 2000) issued a report entitled *Falling Through the Net: Toward Digital Inclusion*. This was the first major U.S. governmental effort to study and document inequalities in access to and use of the internet across social groups. The report showed a trend of increasing usage, but also an increasing gap in usage between urban and rural, minority and non-minority groups, and high and low socioeconomic status households. For some variables, such as gender and income, the gap was decreasing. But the key finding was that 'noticeable divides still exist between those with different levels of income and education, different racial and ethnic groups, old and young, single and dual-parent families, and those with and without disabilities'.

The NTIA report focussed mainly on the U.S., but it did not take long for similar studies to appear that highlighted international aspects of the digital divide. For example, the World Economic Forum (2003) launched its Global Digital Divide Initiative in 2000 'to develop public-private partnerships that would help bridge the

gap between those who have ICT access, skills and resources and those who do not'. The International Labour Organization ([ILO] 2001) released a study in 2001 arguing that lack of access to information and communication technologies (ICTs) on the part of workers in the developing world denied them access to jobs in the technology sector. The report noted that access to ICTs without appropriate education and training would not be a sufficient response to the growing North-South digital divide. Similar studies were done by the World Bank and special agencies of the United Nations.

The Okinawa Charter

At the Okinawa Summit on 22 July 2000, the G8 adopted the Okinawa Charter on Global Information Society. A draft for this document had been prepared for pre-summit discussions with representatives from developing countries at a meeting in Tokyo just before the Summit under the sponsorship of Japanese prime minister Yoshiro Mori. The Japanese government wanted the G8 to go beyond the scheduled discussions of debt relief at Okinawa, partly as a response to the demonstrations against the G8 and the WTO that had taken place in Seattle in 1999 (Chandler 2000).

The Okinawa Charter started by stating that ICTs are 'fast becoming a vital engine for the world economy' (G8 2000). It argued that ICTs have the potential to transform economies and societies because of their 'power to help individuals and societies use knowledge and ideas'. The Okinawa Charter put forward a principle of inclusion in which 'everyone, everywhere should be enabled to participate in and no one should be excluded from the benefits of the global information society'. It stressed the importance of governmental leadership in creating an 'appropriate policy and regulatory environment' that included the fostering of competition and innovation in an overall environment of economic and financial stability. It called for 'collaboration to optimise global networks, fight abuses that undermine the integrity of the network, bridge the digital divide, invest in people, and promote global access and participation'. The last paragraph of the first section of the charter reiterated the G8's commitment to bridging the global digital divide.

The second section of the Okinawa Charter focussed on the need to create the right policy and regulatory environment for ICTs to have a positive impact. The private sector 'plays a leading role' but 'it is up to governments to create a predictable, transparent, and non-discriminatory policy and regulatory environment'. The document went on to stress the importance of enforcing intellectual property rights and liberalising international flows, especially e-commerce. It urged taxation policies consistent with those pursued by the OECD, 'continuing the practice of not imposing customs duties on electronic transmissions', and the adoption of interoperable, market-driven standards. Like the OECD efforts mentioned above, the Okinawa Charter identified privacy protection, electronic authentication, and security as important for future discussion.

The remainder of the document reaffirmed the commitment of the G8 to bridging the global digital divide and suggested ways of working with other international organisations and private sector groups to achieve this goal. In the final pages, the Okinawa Charter announced the decision of the G8 to establish a Digital Opportunity Taskforce (Dot Force) to respond to the needs of the developing countries. The Okinawa Charter became the foundational document for a G8 effort that was to begin in 2000 and end in 2003 with the creation of a number of pilot programmes, reports, and policy dialogues meant to advance the state of art in applying ICTs to development concerns.

The Dot Force

After the Okinawa Summit, 43 teams from organisations representing governments, the private sector, nonprofit organisations, and international organisations were assembled to 'identify ways in which the digital revolution can benefit all the world's people, especially the poorest and most marginalized groups' (Dot Force 2001). The first meeting of the Dot Force was held in Tokyo on 27–28 November 2000, chaired by Japanese deputy foreign minister Yoshiji Nogami. A schedule was established for the preparation of a report prior to the next international economic summit in Genoa. The report, to be finished by May 2001, would be drafted with the help of the World Bank and the United Nations Development Programme (UNDP). It would deal with the issues discussed in the Okinawa Charter and would be 'action-oriented' (Dot Force 2000).

The report that resulted, *Digital Opportunities for All: Meeting the Challenge*, concluded that 'when wisely applied, ICT offer enormous opportunities to narrow social and economic inequalities and support sustainable local wealth creation, and thus help to achieve the broader development goals that the international community has set' (Dot Force 2001). It proposed four areas for action:

- fostering policy, regulatory, and network readiness;
- improving connectivity, increasing access, and lowering costs;
- building human capacity; and
- encouraging participation in global e-commerce and other e-networks.

The members of the Dot Force went so far as to assert that 'basic right of access to knowledge and information is a prerequisite for modern human development'. The enthusiasm for using ICT as the primary vehicle to facilitate access was palpable in the report's verbiage.

The report went on to discuss and summarise the UN Millennium Declaration and the related Development Goals, which included, among other items, reducing the number of people living in extreme poverty by half between 1990 and 2015. It stressed the potential utility of using ICTs to reduce global inequality but also the need to put 'in place the appropriate infrastructure,' which 'is a multi-sectoral and multi-stakeholder

task'. The report referred to the need for governments to work together with nonprofit organisations, private firms, and international organisations. The report claimed that the Dot Force was the first G8 initiative to take this idea seriously. This emphasis on multistakeholder participation was no doubt partly a response to the criticisms of the civil society organizations about their lack of access to decision making in the G8, the WTO, and the World Bank/International Monetary Fund systems.

The report did not ignore the difficulties of the tasks it recommended the G8 to undertake. It included discussions of the problem of general skepticism about the potential role of ICTs in development, opposition to using ICTs to enhance transparency and thereby reduce corruption, and the possibility of negative reactions to the effects of ICT diffusion on employment patterns. It called for fresh thinking on these matters and for a search for best practices on a global basis. The report concluded with nine 'action points' that formed the proposed Genoa Plan of Action. The plan was fully endorsed by G8 leaders at the Genoa Summit in July 2001.

The G8 was led by Italy in 2001 and Canada in 2002. The governments of the two countries were given the responsibility to facilitate the work of the Dot Force after the Genoa Summit. The Dot Force implementation teams proposed a number of new projects in the areas of national e-strategies, access and connectivity, human capacity building, entrepreneurship, ICTs for health, local content and applications, and global policy participation.

These projects and the subprojects associated with them would continue beyond the lifespan of the Dot Force itself, mainly via a hand-off to working groups of the UN's newly created ICT Task Force.

In June 2002, the Dot Force published its final document, entitled *Report Card: Digital Opportunities for All,* in time for discussion at the G8 Kananaskis Summit. This report asserted that the 'multi-stakeholder approach of the DOT Force now serves as the model for other global "ICT for development" initiatives that follow in its footsteps' (Dot Force 2002a, 2). With the conclusion of the Kananaskis Summit, the Dot Force officially ceased operations.

Evaluating the Effectiveness of the Dot Force

The Dot Force was certainly effective in terms of the metrics devised by John Kirton (2004) to evaluate the overall effectiveness of other G8. The task force generated lots of paper, there were many attendees of meetings, and there were a number of substantial financial commitments on the part of the G8. But its main accomplishment seems to have been experimenting successfully with a different way of operating. Unlike previous G8 initiatives, the Dot Force consciously employed a multistakeholder approach, in which government officials worked together with representatives of private

firms, nonprofit organizations, and international organisations to write reports and propose new projects to be funded by a combination of governmental, intergovernmental, and private sources. The fact that the OECD appears to be adopting such an approach in dealing with e-commerce issues is not a coincidence.

It is probably still too soon to evaluate the effectiveness of the Dot Force projects, but they at least had the appearance of originality and careful thought that is not always characteristic of development projects. Another hopeful sign was the tempering of the ambitions of a few overly enthusiastic advocates of ICTs and the replacement of unrealistic notions with more realistic ones. A particularly poignant example of this is the network of public internet access points (ADEN, or Appui au désenclavement numérique) sponsored by the French government. ADEN would create shared access points to the internet in Africa in public locations and with local community associations as partners. To deal with the many interruptions in power and telephone services and the high cost of connectivity in Africa, these access points would employ a technology using short bursts of interconnection for storage of information most likely to be needed at the access point.

Similarly, a passage from the part of the report card summarising the work of the human capacity team shows how their collective thinking about how to apply e-learning technologies in the developing world influenced (mostly for the good) the technological enthusiasts among them:

> The team realizes the need for a more adjusted and differentiated view of the potential associated with the implementation of ICTs in low-income countries. It is also aware of excluding vast majorities from this potential. Meeting these particular needs should enable a more fruitful discussion with critics who perceive the issue — in light of the often overwhelming problems of hunger, water scarcity, and physical threat — as a diversion from basic development needs. It should also, and more importantly, foster sustainable, bottom-up developments and applications that take advantage of basic and enhanced ICTs to improve the living conditions of all citizens (Dot Force 2002b, 4).

The entrepreneurship team was different from the others in asking for US$32 million from the G8 governments to create the Dot Force Entrepreneurial Network (DFEN). The DFEN would focus on financially supporting small- and medium-sized enterprises engaged in ICT activities in the developing world. The DFEN was renamed Enablis in 2002 after it received CA$10 million (about US$6.6 million) in funding from the Canadian government. It is sponsored in addition by three private firms that were involved in the entrepreneurship task force of the Dot Force: Accenture, Hewlett-Packard, and Telesystem. Enablis planned to set up a regional office in South African in the fourth quarter of 2003, with two satellite offices in Africa by the end of 2004 (Enablis 2004).

The Shift to Cybersecurity Issues

Immediately after the attacks on the World Trade Center and the Pentagon on 11 September 2001, the G8 leaders shifted their attention away from issues such as those discussed in the Dot Force toward cyberspace issues related to security ('cybersecurity' for short). The G8 had begun already to consider these issues prior to 11 September, having created the Senior Experts Group on Transnational Organized Crime (later renamed the Lyon Group) in 1995 at the Halifax Summit. The experts group presented its first report at the G8 Summit in Lyon, which included recommendations for reviewing 'their laws in order to ensure that abuses of modern technology that are deserving of criminal sanctions are criminalized and that problems with respect to jurisdiction, enforcement powers, investigation, training, crime prevention and international cooperation in respect of such abuses are effectively addressed' (P8 Senior Experts Group 1996, 4). They were given an open-ended mandate to implement the proposed recommendations. Since then, the Lyon Group has developed into a permanent, multidisciplinary body helping to provide information for meetings of the G8 justice and interior ministers.

In October 1999, the G8 justice and interior ministers authorised a Lyon Group meeting on Confidence and Security in Cyberspace to be held in Paris in May 2000. There was a follow up meeting in Berlin in October of that year. A third conference was held in Tokyo in May 2001. The agenda of the Tokyo meeting including the issues of data retention, data preservation, threat assessment and prevention, protection of electronic commerce, and user authentication and training. After 11 September, the Lyon Group was given the initiative to devise methods for detecting and intercepting international transfers of funds for the purpose of supporting terrorism. Its purview also included consideration of methods to detect and prevent money laundering, an issue that became particularly relevant after information about funding of al Qaeda operations was made public (G8 Lyon Group 2002; Miyake 2001). The Lyon Group also pushed successfully for the adoption of the UN Convention against Transnational Organized Crime on 15 November 2000 (UN General Assembly 2000, Annex I).

At the G8 Summit in Paris in 1989, the Financial Action Task Force (FATF) was set up to co-ordinate G8 policies with regard to international money laundering. The FATF came to have 33 members by 2003, most of them members of the OECD but also including some Latin American countries, the Gulf Cooperation Council, and the EU.[2] In 1996, the FATF issued 40 recommendations on money laundering that was modified and expanded after 11 September 2001 under the leadership of the G8, to include eight recommendations on the financing of terrorism (FATF 2003b).

While the FATF recommendations included policies directed at electronic funds transfers, the main concern in the area of terrorist finance was informal money transfer networks such as the hawala networks used in Islamic banking, where international payments are made via linked money swaps that defy international monitoring.[3] Nevertheless, since June 2000 the FATF has maintained a list of Non-Cooperative

Countries or Territories (NCCTs) that includes large countries such as Nigeria and small island republics such as Nauru and the Cook Islands that are notorious not just for money laundering but also for serving as shelters for all kinds of illicit Internet and email scam operations (see Chapter 12).

The governments of Western Europe, North America, and Japan adopted a variety of policies to respond to a heightened level of threat after 11 September, some of which would directly influence the G8's future deliberations on cyberspace governance. In June 2001, the European Commission (2001) issued a document entitled 'Communication on Network and Information Security', which outlined an approach to security on computer networks that included policies to deal with cyber-attacks, identity thefts, attacks on infrastructures, and other types of cyber-crime. The document stressed the importance of raising consciousness about these matters and of establishing computer emergency response teams (CERTs) in member states. It highlighted the importance of standards for electronic signatures (authentication), encryption, and interoperability, and called for greater international co-operation in this area.

In 2002, the European Union adopted its e-Europe 2002 Action Plan, which included a number of proposals for policies for maintaining cyber-security. The European Union subsequently issued the Electronic Signatures Directive and launched the European Electronic Signature Standardization Initiative to help companies implement the directive. The EU endorsed the Council of Europe's 1990 Convention on Cybercrime and proposed its own Framework Decision on Child Pornography, which included provisions to prevent the exchange of child pornography over the internet. The European Commission established a European network of hotlines under the Safer Internet Action Plan to ease the reporting of illegal internet content, including child pornography. In February 2003, the EC proposed the establishment of the Network and Information Security Agency. This agency would co-ordinate and assist the CERTs of EU member states and help to raise awareness of the dangers of cybercrime and the need to adopt appropriate countermeasures.

The U.S. government established the Department of Homeland Security (DHS) after 11 September, which included among its many new sub-agencies the National Cyber Security Division. In September 2003, a former vice-president of Symantec Corporation became the director of this division. At about the same time, DHS Secretary Tom Ridge announced the creation of a U.S. CERT in co-operation with Carnegie-Mellon University (Ferrell 2003). In Japan, an Information Technology Security Office was established in the Cabinet Secretariat to develop countermeasures against cyber-attacks and to protect e-government operations. The office was given the lead in co-ordinating the government's various cyber-security efforts. In a joint statement, the governments of the two countries announced that they were considering becoming parties to the Council of Europe's 1990 Convention on Cybercrime (U.S. Embassy in Tokyo 2003).

To summarise, the most important activities of the G8 during this period were those undertaken within the Lyon Group and the FATF. But the broader array of cyber-

security issues — which included, among others, laws, technologies, and technical standards to prevent cyber-attacks, infrastructure attacks, identity thefts, and the exchange of child pornography — would clearly be on the G8's agenda in the future.

Conclusion

In conclusion, the Dot Force, the FATF, and the Lyon Group demonstrated the potential effectiveness of the G8, especially relative to other international regimes, in creating solutions to collective action problems in cyberspace. The main problem that the Dot Force solved was providing an answer to antiglobalisation critics of the tendency of intergovernmental organisations such as the G8 to exclude participants from civil society — that is, private firms, nongovernmental organisations (NGOs), and other social groups. As to how the various Dot Force projects would do in bridging the digital divide, only time would tell. Nevertheless, the new collaborative approach embodied in the multistakeholder model was bound to be more successful than the purely intergovernmental approach because it permitted the G8 to tap directly some of the best ideas of participants in civil society with greater knowledge than the government officials that normally participated in G8 deliberations.

Similarly, the Lyon Group provided an excellent foundation upon which to build a credible G8 response to 11 September. The participation of private sector interests in the Lyon Group was partly responsible for its success, even when the main work was done by law-enforcement agencies of G8 governments. Even in primarily security-related areas of the G8's work, it has become necessary for the intergovernmental essence of the G8 to be modified so that the resources of members of civil society can be added to those of G8 governments to solve important collective action problems.[4]

It should be noted, however, that the only reason the G8 was able to pursue these experiments with multistakeholder participation in discussing governance issues was its original stress on 'heads only' or at least 'heads primarily' in G8 meetings. That is, since the G8 had started with the idea that a periodic assembling of heads of state without too much representation of cabinet or sub-cabinet level officialdom was the best way to resolve the most important issues, there was always some flexibility to invite nongovernmental parties to participate in G8 discussions. More formally organised intergovernmental organisations are generally less able to do this.

There is always a danger of overstating the benefits of incorporating civil society actors in international governance because, at least in some cases, civil society may not be well represented in the entities claiming to do so. Because of their superior financial resources, private firms (and particularly large private MNCs) may be able to plead for special treatment in ways that are contrary to the public interest. They may 'capture' the public or quasi-public governance institutions to the detriment of other members of civil society. The same can occur for transnational environmental groups, labour organisations, or international financial institutions. Thus, one must be

skeptical about general claims about the superiority of the multistakeholder approach to international governance. Nevertheless, in areas, such as internet governance, where private actors are needed both to provide accurate informational inputs to form and implement new norms, rules, and procedures, a properly configured multistakeholder approach is both necessary and desirable.

Notes

1. The document bears the names of both President William Clinton and Vice-President Albert Gore.
2. For a list of members, see FATF (2004).
3. See, for example, FATF (2003a). Such informal money swaps do not require computers or telecommunications technology and can be arranged via telephone or fax.
4. Nicholas Bayne has argued in this volume and elsewhere that the 'heads only' aspect of the G8 permits it to have the flexibility to do this whenever the heads of state so desire.

References

Beaird, Richard (2003). 'Opening Remarks'. OECD-APEC Forum: Policy Frameworks for the Digital Economy, 14–17 January. Honolulu. <www.oecd.org/dataoecd/19/56/2492657.pdf> (November 2004).

Chandler, Clay (2000). 'In Tokyo, Rich Pay Heed to the Poor as G8 Summit Opens'. *Washington Post*, 21 July, p. A19.

Digital Opportunity Task Force (2000). 'First Meeting of the G8 Digital Opportunity Task Force'. 30 November. <www.g8.utoronto.ca/dot_force/summary-nov-00.html> (November 2004).

Digital Opportunity Task Force (2001). 'Digital Opportunities for All: Meeting the Challenge. Report of the Digital Opportunity Task Force (DOT Force) Including a Proposal for a Genoa Plan of Action'. <www.g8.utoronto.ca/summit/2001genoa/dotforce1.html> (November 2004).

Digital Opportunity Task Force (2002a). 'Report Card: Digital Opportunities for All'. <www.g8.utoronto.ca/summit/2002kananaskis/dotforce_reportcard.pdf> (November 2004).

Digital Opportunity Task Force (2002b). 'Team Report: Human Capacity and Knowledge'. Ottawa, June.

Enablis (2004). 'Enablis in Brief'. <www.enablis.org> (November 2004).

European Commission (2001). 'Network and Information Security: Proposal for a European Approach'. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee, and the Committee of the Regions. <europa.eu.int/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf> (November 2004).

Ferrell, Keith (2003). 'Homeland Security Getting Its House in Order'. *Security Pipeline*, 17 September. <www.securitypipeline.com/news/showArticle.jhtml?articleId=14800063> (November 2004).

Financial Action Task Force (2003a). 'Combating the Abuse of Alternative Remittance Systems: International Best Practices'. 20 June. Paris. <www.fatf-gafi.org/pdf/SR6-BPP_en.pdf> (November 2004).

Financial Action Task Force (2003b). 'The Forty Recommendations'. Organisation for Economic Co-operation and Development, Paris. <www1.oecd.org/fatf/40Recs_en.htm> (November 2004).

Financial Action Task Force (2004). 'Members and Observers'. <www.fatf-gafi.org/Members_en.htm> (November 2004).

G8 (2000). 'Okinawa Charter on Global Information Society'. Okinawa, 22 July. <www.g8.utoronto.ca/summit/2000okinawa/gis.htm> (November 2004).

G8 Lyon Group (2002). 'The G8 Lyon Group'. <www.auswaertiges-amt.de/www/en/aussenpolitik/vn/lyon_group_html> (November 2004).

Global Information Infrastructure Commission (1995). 'GII Commission Inaugural Meeting'. World Bank, 11–12 July. Washington DC. <www.giic.org/events/ann1.asp> (November 2004).

Hart, Michael, François Bar, and Robert Reed (1992). 'The Building of the Internet: Implications for the Future of Broadband Networks'. *Telecommunications Policy* vol. 16 (November), no. 666–689.

Information Society Website (1995). 'G7 Information Society Conference'. 25–26 February. Brussels. <europa.eu.int/ISPO/intcoop/g8/i_g8conference.html> (November 2004).

International Labour Organization (2001). 'World Employment Report 2001: Life at Work in the Information Economy'. Geneva. <www.ilo.org/public/english/support/publ/wer/index2.htm> (November 2004).

Kirton, John J. (2004). 'Explaining G8 Effectiveness: A Concert of Vulnerable Equals in a Globalizing World'. Paper prepared for the International Studies Association conference. Montreal, 17–20 March. <www.g8.utoronto.ca/scholar/kirton2004/kirton_isa_040304.pdf> (November 2004).

Miyake, Kuriko (2001). 'G8 Concludes Tokyo High-Tech Crime Meeting'. CNN, 21 May. <archives.cnn.com/2001/TECH/internet/05/31/g8.cyber.crime.idg> (November 2004).

National Telecommunication and Information Administration (2000). 'Falling Through the Net: Toward Digital Inclusion'. United States Department of Commerce. <www.ntia.doc.gov/ntiahome/fttn00/contents00.html> (November 2004).

Organisation for Economic Co-operation and Development (1998). 'A Borderless World: Realising the Potential of Global Electronic Commerce'. Organisation for Economic Co-operation and Development, Paris.

Organisation for Economic Co-operation and Development (2000). 'E-Commerce: Implementing the Ottawa Taxation Framework Conditions'. Report to Ministers, C/MIN (2000)9. <www1.oecd.org/subject/mcm/2000/e_comm_ott.pdf> (November 2004).

Organisation for Economic Co-operation and Development (2003a). 'Implementation of the Ottawa Taxation Framework Conditions: The 2003 Report'. Paris. <www.oecd.org/dataoecd/45/19/20499630.pdf> (November 2004).

Organisation for Economic Co-operation and Development (2003b). 'Privacy Online: OECD Guidance on Policy and Practice'. Paris. <www1.oecd.org/publications/e-book/9303051E.PDF> (November 2004).

P8 Senior Experts Group (1996). '40 Recommendations to Combat Transnational Organized Crime'. April, Paris. <www.auswaertiges-amt.de/www/de/ infoservice/download/pdf/vn/g8_recommandations.pdf> (November 2004).

Rotenberg, Marc (2003). 'Global Forum on Information Systems and Networks Security: The Role of Civil Society'. Oslo, 13–14 October. <www.oecd.org/dataoecd/25/19/17842138.pdf> (November 2004).

Skantze, Pernilla (2003). 'European Cyber Security'. OECD Global Forum on Information Systems and Network Security: Towards a Global Culture of Security. <www.oecd.org/dataoecd/53/43/17979495.pdf> (November 2004).

Smith, Marcia S., John D. Moteff, Lennard G. Kruger, et al. (2001). 'Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth'. 31 January. CRS Report for Congress. <www.4uth.gov.ua/usa/english/tech/reports/98-67.pdf> (November 2004).

United Nations General Assembly (2000). 'Crime Prevention and Criminal Justice: Report of the Ad Hoc Committee on the Elaboration of a Convention against Transnational Organized Crime'. A/55/383. 2 November.

United States Embassy in Tokyo (2003). 'U.S.-Japan Joint Statement on Cyber Security'. 9 September. <japan.usembassy.gov/e/p/tp-20030909d2.html> (November 2004).

White House (1997). 'A Framework for Global Electronic Commerce'. 1 July. <www.technology.gov/digeconomy/framewrk.htm> (November 2004).

World Economic Forum (2003). 'Global Digital Divide Initiative'. <annualmeeting.weforum.org/site/homepublic.nsf/Content/Global+Digital+Divide+Initiative.html> (January 2003).