"CUIUS REGIO, EIUS RELIGIO, OMNIUM SPATIUM?" STATE SOVEREIGNTY IN THE AGE OF THE INTERNET

Giampiero GIACOMELLO and Fernando MENDEZ

1. Introduction

The belief that sovereignty is at the eleventh hour has become more widespread with the progress of the globalization phenomenon. The notion that sovereignty is somehow being transformed by the process of economic globalization and that this is being exacerbated by the Internet—one of the cutting-edge tools of globalization—has become an almost uncritically accepted fact. Large swathes of public opinion in industrialized democracies have been mesmerized by the pervasive equation that more globalization (and more Internet) equals less sovereignty. In this article we attempt to dissect the proposition that more Internet equals a further decrease in state sovereignty. We argue that, while state sovereignty is unmistakably declining, the Internet is, in the best case, one more element contributing to that decline. Indeed, in some instances the Internet can even strengthen sovereignty.

In this article we address the question of whether and how the Internet is affecting/changing states' sovereignty. Our article for this special issue of *Information and Security* is best conceived as a "plausibility probe."[1] The purpose of such a study is to enable the investigator to judge whether the potential validity of the explanatory hypothesis (or hypotheses) is large enough to justify a greater effort to produce more decisive hypotheses-testing studies.[2] The fact that the Internet is still somewhat of an unknown topic in many disciplines (including security studies) ensures that any exploratory investigation must proceed with inductive logic. This will allow us to enhance our conceptual tools with the ultimate goal of producing more systematic hypotheses in further studies.

Sovereignty (from the Latin word *super*, above) basically means authority. The notion was first developed by Jean Bodin (1530-1596) and Thomas Hobbes (1588-

1679), who identified it with the authority emanating from the sovereign. More recently, sovereignty has been defined as "... the claim to be the ultimate authority, subject to no higher power as regards the making and enforcing of political decisions. In the international system, sovereignty is the claim by the state to full self-government…."[3] Sovereignty has simultaneously an internal and an external significance, since the concept implies autonomy in foreign policy and exclusive competence in internal affairs.[4] The former attribute is thus indispensable to be a member of the international society of states; while the latter means that that authority is limited/circumscribed by borders (beyond which lays the sovereignty of others) and can be exercised only over the population residing within those boundaries. Scholars have traced the origins of the concept to the Treaties of Westphalia (Münster and Osnabrück) which, in 1648, concluded the Thirty Years War (the title of this article is an explicit reference to the religious diversity also established by the treaties). The treaties established "… a secular concept of international relations replacing forever the medieval idea of a universal religious authority acting as the final arbiter of Christendom."[5] Consequently, from 1648 onwards, the particularistic interests of states became paramount both politically and legally. Given the unconditional authority that characterized the Westphalian conception of the nation-state and sovereignty, it is not surprising that an erosion of sovereignty has been steadily accruing over the centuries. In the end, the diffusion of the Internet is seen by futurologists and many technologists as a "lethal" instrument for states' authority.

2. Towards a Conceptual Framework

The contemporary debates concerning the Internet and sovereignty are characterized by what appears to be an uncanny paradox. While the new Internet technologies favor speed and decentralization, one of the most salient features of the political systems, in which they operate, is that they are simply not set up in this way. Politics tends to be a slow and consensus seeking business, it is usually characterized by uncertainty and an incredible sensitivity to particular interests. How these conflicts are resolved will have a major impact on the development trajectory of the Internet. These two conflicting dynamics are encapsulated by two radically different perspectives on the Internet.

On the one hand, the engineer/technologist perspective, views the Internet as an astonishingly elegant and seamless global information network that transcends national borders. It is because of this transnational technological attribute that the ability of nation states to regulate or control the Internet is severely curtailed, this logically entails an erosion of sovereignty. On the other hand, a regulator perspective, offers a stark contrast. Seen from this perspective, the cyberworld is presently in an anarchic state of nature. Major regulatory fault lines are emerging in relation to areas

such taxation, applicable law, copyright and content, to name but a few. Political solutions to this regulatory "chaos" will have to be negotiated and to the extent that nation-states are able to create adequate regulatory regimes this does not necessarily entail an erosion of sovereignty.

There is of course an obvious danger in polarizing what is an infinitely more complex picture. The research design and conceptualization adopted in this article is intended to principally serve as a heuristic device, it can subsequently form the basis for a more rigorous and systematic formulation of hypotheses. It is an attempt to provide a "photo-type" picture of the current state of affairs concerning the interaction between emerging digital technologies and our institutions of governance. What are the regulatory outcomes that are being produced by this interaction as policymakers respond to the challenges posed by the Internet? Has the technological juggernaut constrained policy-makers options? If this is so then one can justifiably refer to an erosion of sovereignty. Or is the nation-state adapting to this new environment and, if so, with what results?

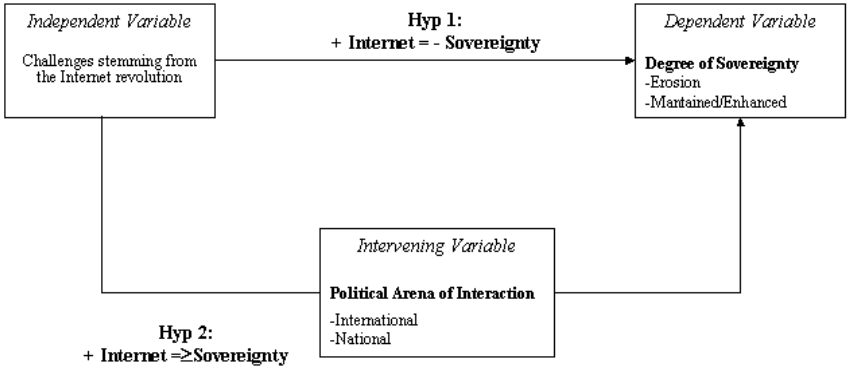
One way in which this adaptation process works is through the mediation of disparate interests within the arenas of political interaction. The proliferation in the use of the Internet has mobilized a whole host of actors into strategic political action. These actors, ranging from business organizations and civil liberties groups to policy-makers and law enforcers, interact in different political arenas to achieve their desired goals. The outcome of these interactions usually takes the form of new rules. As new rules are created by assigning property rights, by constraining actors choices and by prescribing who can act and when, a regulatory regime begins to emerge and will affect behavior both directly and indirectly. The creation of these rules, which vary across various dimensions of formality and specificity, are central to any discussion of governance and sovereignty. Is it conceivable that as new regulatory regimes emerge, both at the international and supranational levels, states can actually enhance, or at least not suffer a serious diminution of sovereignty? In setting up the problem we are interested in examining the role of the political arena, be it national or international, in shaping regulatory outcomes.

3. Hypotheses and Variables

We can now proceed to translate these ideas into a simple causal argument using the language of variables. These can subsequently form the basis for a set of rival hypothesis that posit distinct outcomes. Our dependent variable is *changes in sovereignty*, and we wish to explain the extent to which the new Internet technologies are producing erosion in states' sovereignty. *Internet technologies* are, therefore, our independent variable. We however add another variable to the analysis, which we have referred to as the *political arena of interaction*. This acts as an intervening

variable, and it has a mediating affect between the independent and the dependent variable. Does this intervening variable have a significant effect on regulatory outcomes? Can it be ignored or treated as a residual?

The aim of this—admittedly very simplistic set up—is to attempt to test for the role of the political arena. The simplicity of this set up however is justified by the purpose of this article, which is to be an "exploratory" study on this still rather indefinite and debated topic of Internet and state sovereignty. Having identified the key variables we can now postulate two rival hypotheses that differ with regard to the outcomes (see the diagram).



1) The "techno-driven" or "general belief" hypothesis: the more the Internet grows, the more sovereignty is eroded. Futurologists and large portion of the informed public (the so-called "digerati") share this view. They maintain that technology has a strong *direct* influence on policymakers' ability to pursue independent policy. Most techno-driven hypotheses share a similar diagnosis of the futility of attempting to steer technical change. Nicholas Negroponte,[6] one of the Information Age gurus, offers a "rosy" version of the techno-driven thesis. As we move away from the "atom" society to the 'bit' (i.e. digital) society the structure of society, the economy and current forms of political organization will be transformed.

One of the chief victims will be the nation-state, which will be unable to withstand the decentralizing, globalizing, and empowering potential of digital technologies. Others, such as Angell,[7] while agreeing with Negroponte as to the irrelevance of political institutions offer a much darker prognosis in which mass unemployment and anarchy will prevail. The defining characteristic of these techno-driven approaches is that they all share a similar conception of the main agent of change and the powerlessness of

institutions in the face of technological imperatives. They all point to an erosion of sovereignty.

2) The "politics matters" hypothesis: Internet growth does not inevitably translate into decrease in state sovereignty. It can even lead to an increase. It thus becomes paramount to analyze the "politics" of the Internet growth. This "institutionalist" view does not necessarily treat the technological change as unimportant; rather the influence of that change will be heavily filtered by domestic political and institutional structures.

Policy responses will reflect certain cultural values. There may be a greater likelihood of international conflict in the political economy of the Internet arising, for instance, as a result of differing views as to the role of governments. It may also arise from the way in which interests are articulated within different political systems. Such analyses put the institutional and political framework at the core of the analysis.[8]

4. Cases

To support our argument, hereafter we present four examples of decrease (-) or no-change/increase (≥) in sovereignty. One example of a decrease, online tax (-) and one example of a no-change/increase (≥), Yahoo!. Furthermore, in order to maximize variation on our dependent variable we provide two additional examples, Domain Names and the management of the Internet and cybercrime. These contain elements that can be viewed both as a decrease and an increase in sovereignty. We have selected the cases on the basis of variations of our dependent variable (changes in sovereignty), which is a well-known procedure in social science methodology.[9]

4.1 Domain Names and the Management of the Internet

Since its origins, the Domain Name System (DNS) has determined on-line identities. Clearly, the DNS is vital for the private sector, where brands and trademarks are the key to business success. Companies want their names to be recognized worldwide—including the World Wide Web—and do not want unknown individuals to illegally exploit or meddle with their reputation. On the basis of a Memorandum of Understanding signed with the US Department of Commerce in October 1998 a new organization was born—the Internet Corporation for Assigned Names and Numbers (ICANN)—a non-profit, private sector corporation formed by a broad coalition of the Internet's business, technical, academic, and user communities.

ICANN, along with other similar governance organizations such as the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF) have since become the closest thing that there is to an "Internet government."[10] It appears that governments have surrendered considerable authority to these new organizations,

which can powerfully influence Internet development. This in turn can lead to further erosion of state sovereignty. In the case of the W3C, for instance, governments can have the status of "members" just like a corporation or an NGO, with no special privileges attached. This process of "U.N.ization" of the Internet seems to confirm the futurologists' explanation and the general belief that the spreading of the Internet inevitably implies a reduction of states' authority.

This interpretation is only partially correct. In fact, states do "fight back" the loss of sovereignty. EU governments, for instance, have only reluctantly embraced the "privatization" process of the DNS, adopted (to some extents, imposed) by the United States, where the public tends to see the reduction of the federal state's involvement as a positive development. In fact, EU member states have tried to reverse the process, limiting ICANN's unaccountability and independence. The near-adoption of a *.eu* extension for Europe, excluded from ICANN interference is an indication of such attitude.

Other states—including less democratic ones—have adopted the same attitude. China, for instance, has undertaken a "tug-of-war with Western domain-name monitoring and registration firms over who has control of Chinese-language Internet naming rights."[11] The China Internet Network Information Center (a government agency) on 18 January 2000 initiated Chinese domain-name testing system with suffixes of Chinese-language counterparts of .cn, .com, and .net. Western registration organizations have claimed that such decision can pose a threat to the uniformity of Internet addresses. The Chinese government is thus trying to prevent Western influences and business advantage while, at the same time, preserve its freedom of action with censorship. Ultimately, "... the issue has risen alarmingly to the level of a dispute over national sovereignty rather than simple registration activity and concerns over commercial interests."[12]

4.2 Yahoo!

A recent example of a nation state asserting itself concerns the French Yahoo! Court case. It is likely to have important repercussions and has led to an important debate with regard to the governance of the Internet. In April 2000, three anti-racist and Jewish associations (Licra, Mrap and UEJF) lodged a complaint against Yahoo! before a French Court for hosting online auctions of Nazi memorabilia. French law prohibits the exhibition of objects that incite racial hatred. The Court case could be interpreted as something of a test case to see who has the power, and confidence in their legal system, to attempt to regulate aspects of the Internet. [13]

The issue arose in the context of a growing anti-globalization backlash and, in France, was allied with a general perception of the invasion of American culture.

Conversely, on the other side of the Atlantic it was seen as yet another manifestation of French intransigence. In France, it was portrayed as a case of whether a nation-state can regulate within its jurisdiction, i.e. prohibit unlawful content, or whether it has to be subject to a set of lowest common denominator laws, i.e. the freedom of speech laws of the US that permit such activity. The French courts decided to hold Yahoo! responsible and gave it three months to block access to the US auction site. A raging debate ensued amongst interested parties as to the merits/flaws of the decision. Yahoo! initially argued that it was impossible to filter every piece of information. Nevertheless, in January 2001 as the profit implications and bad publicity for the company in a lucrative market sank in, it agreed to block the sale of Nazi memorabilia on its auction sites, in effect capitulating to the extraterritoriality of the French Court. The self-censorship marked a significant U-turn by the US portal, which had previously opposed the principle that it should block access. [14]

In a rather prophetic article that was written before the Yahoo!-case, Goldsmith [15] had set out the reasons why unilateral actions were likely to be a much more frequent attribute of the governance of the Internet and the conditions in which it would be successful. He argued that governments can take significant actions to regulate the flow of items within its borders, i.e. by imposing cost on persons and properties within its territories. This could take the form of punishing local assets of foreign content providers or penalizing in-state end-users who obtain foreign content. Although governments will not be able to eliminate all individual transactions they can significantly raise the cost of the activity in question to achieve their desired goals. This is precisely what occurred in the Yahoo!-case. Such events are beginning to explode the myth of the borderless nature of Internet as well overturning some of the more utopian Internet pioneer's "information libertarianism" whose unifying ideal was a desire for unfettered information flows and opposition to any forms of censorship.

4.3 Taxation on the Internet

"No taxation without representation" was a motto of the American Revolution, which implied that the imposition of taxes without proper laws passed in a parliament representing the local constituency was a despised manifestation of absolute monarchs. Indeed, since the origins of the modern state, imposing taxes has been one of the most distinctive features of sovereignty. Although, thus far, electronic commerce is still only a fraction of global trade, governments fear that that prerogative of state power could be severely limited by the fast growth of electronic commerce and began to consider ways in which to tackle such a prospect.

Tax imposition can only work within the precise limits of a state's boundaries. The Internet, among other roles, is also an "international trade route,"[16] thus requiring

special treatment in terms of taxation (as well as law enforcement, etc.). Quite unsurprisingly, "... the United States Treasury Department has identified the tax ramifications of such high-technology issues as transactions over the Internet as a 'top-priority' international issue ...."[17] Last but not least, to make their action even more problematic, states still use mid-twentieth century tax systems—designed largely for manufacturers and vendors of tangible personal property—to tax a technologically advanced 21st century service industry.[18]

National governments are by no means powerless: they can still track resident individuals and physical goods and tax them. However, several products are already available in digital format (from music to books to films), and this tendency will only increase in the future. It is difficult if not plain impossible (especially if they are all encrypted) to monitor the traffic of these products. The situation is even more manifest with services (including moving money tax avoidance and other criminal shifting of income), which hardly leave traces. Finally, the extreme variety and span of national tax systems makes it extremely problematic to yield international treaties that would satisfy all parties.[19] Nowhere is this more the case than with the current Internet tax state of affairs.

On the one hand, the US wants to maintain the current Internet tax moratorium, while on the other hand the European Commission is keen to apply VAT to Internet transactions. These differences will need to be ironed out and will be subject to intense negotiations. Nonetheless, there is no doubt that the Internet "... presents a serious informational and enforcement crisis to revenue authorities."[20] If governments cannot find a proper mode to answer this challenge, the erosion of the tax basis in the long run could fatally undermine the very existence of state sovereignty.

4.4 Cybercrime

The cybercrime example is illustrative of the interaction between technologies and issues of sovereignty. On one hand, cyber criminals have the potential to operate globally, while on the other hand, prosecuting agencies are bound by the principle of national sovereignty and are limited by national territory, which can only be overcome by slow and bureaucratic means of mutual assistance. Thus, in relation to cybercrime this contradiction makes international and supranational solutions indispensable since the non-coordination of national strategies could result in the proliferation of cybercrime havens. At the heart of the policy is the challenge to ensure basic rights, i.e. privacy and anonymity, while permitting restrictions to these rights in certain circumstances. How is this balancing act being negotiated?

To date some of the measures adopted to combat the potential for cybercrime by some countries have inflamed civil liberty groups both in the US and in the EU. The

Regulation of Investigatory Powers Act [21] in the UK and the FBI's development of the Carnivore program [22] in the US are clear examples of the privacy concerns raised by legislation and the advances in technology that enhance the surveillance powers of nation-states. Is it possible that by coming together, through multilateral frameworks, nation states can actually enhance aspects of their sovereignty?

The international arena, however, poses problems with regard to issues such as sovereignty and cultural diversity as well as very different traditions of criminal law. To date there has been a degree of international activity on the issue of cybercrime, of which the most significant examples include the G8 Recommendations [23] and the OECD guidelines.[24]

By far the most important multilateral coordination is taking place at the Council of Europe (CoE), which in 1997 began negotiations to draft a treaty on cybercrime. The drafting process was conducted in a closed and secret environment with the first public draft only released in April 2000.[25] The CoE *Draft Convention on Cyber Crime* will be a defining text given that it will constitute the first international treaty on cybercrime. It is based on the premise that the risks related to cybercrime need to be addressed at the international level and, to this end, aims to create a world benchmark or minimum standard in the fight against cybercrime. Indeed, many non-European countries such as the US, Canada, Japan and South Africa actively participate in the drafting process. Most importantly, the process sets itself apart from what is occurring at other international forums such as the G8, OECD and the United Nations due to its binding nature. The draft, as it stands, aims to a) harmonize legislation on what constitutes a cybercrime, i.e. the substantive law issues; b) enhance investigative procedures, i.e. procedural law issues; and c) to develop closer international cooperation.

The aspect of the Treaty, which is most controversial given its enormous implications for privacy, is the section that deals with procedural law, i.e. interception of communications and seizure of computer data by governments. These investigative powers issues have inflamed civil liberties groups and business organizations. For instance, the Center for Democracy and Technology (CDT)—a respected Washington D.C. based civil liberties group—has condemned the unbalanced nature of the Treaty which includes very detailed procedures for interception and seizure mechanisms without any corresponding privacy standards or real limits to government powers.[26] CDT has pointed out the paradoxical nature of the draft, which is not "focused on viruses, hacking or other attacks against computer systems or the computer-dependent critical infrastructures. Instead, central provisions of the Treaty are intended to require governments to adopt laws on search and seizure of computer evidence, disclosure to governments of computerized records of any kind, and electronic interception of communications—*for all kinds of crimes*."[27]

In other words, the major focus of the Treaty is on enhancing the surveillance potential for law enforcement agencies through increased investigative powers. This has led some civil liberties groups to claim that the FBI is using a foreign forum to create an international law enforcement regime.[28] There is certainly some force to this argument given the role of the US Justice Department in the drafting process.

Law enforcement/security agencies have been mobilized into seeking preemptive action, or creating a favorable rule regime to enhance their surveillance and interception powers (not just for Internet crimes but also as a means of combating traditional crimes). The preferred arena, given the nature of the problem, is the international level. At the same time, however, another group of actors pursuing very different agendas have been mobilized to counteract the demands of the law enforcement/security agencies, which are deemed to pose either draconian privacy intrusions or disproportionate financial burdens.

The outcome of these battles between rival interests will be largely determined by the power relations between the competing organizations and the set up of the political arena in which the rules are created. Thus, the political arena can provide for varying degrees of access to power for the respective organizations. For instance, in the case of the CoE Draft Cybercrime Convention the law enforcement/security agencies—given that they had a fist mover advantage—were able to play a dominant role in the drafting of the Treaty text. They therefore played a crucial role in the agenda-setting process.

5. Conclusions

To review the central argument and by way of conclusion let us briefly revisit the hypotheses. We have argued that the simplistic proposition that more Internet equals less sovereignty seriously underestimates the ability of the nation state to adapt to a given technological reality. Thus, all we claim, at this early stage, is that nations do seem to be responding and that these responses will tend to have an influence on the development trajectory of the Internet. Whether developments in the technological domain will find a way to circumvent onerous policy decisions is, for the moment, a separate research question. The serious research agenda is to explain the conditions in which a nation state can assert itself and those where it is more difficult.

Our Yahoo! and cybercrime examples demonstrate that under certain conditions, i.e. where a nation state can punish an alleged transgressor's asset base or where agents of the nation state such as law enforcers enjoy agenda setting powers, the simplistic view of the techno-driven hypothesis begins to breaks down. Conversely, the taxation and ICANN examples are illustrative of instances where sovereignty can be called into question. Nevertheless, even in these latter cases it seems that the nation state

may have more room for maneuver than is commonly assumed. The increasing politicization of ICANN's organizational structure and looming transatlantic differences with regard to online taxation suggest that politics still matters. The simplistic equation that we set out to examine should be reformulated along the following—equally simplistic but perhaps more accurate—lines: More Internet equals more politicization. We believe that examining the nature of this politicization, and the conditions in which it entails an erosion of sovereignty, constitutes a much more fruitful research agenda.

Notes:

1 Harry Eckstein, "Case Study and Theory in Political Science," in *Handbook of Political Science, vol. 7: Strategies of Inquiry*, ed. Fred Greenstein and Nelson Polsby (Reading MA, et al.: Addison-Wesley, 1975), 79-137.

2 Alexander L. George, "Case Studies and Theory Development: The Method of Structured, Focused Comparison," in *Diplomacy: New Approaches in History, Theory and Policy*, ed. Paul G. Lauren (New York: Free Press, 1979), 43-68.

3 Barry Buzan, "Sovereignty," in *The Concise Oxford Dictionary of Politics*, ed. Iain McLean (Oxford and New York: Oxford University Press, 1996), 464.

4 George Evans with John Newnham, *Dictionary of International Relations* (London: Penguin Books, 1998), 504.

5 Evans, *Dictionary*, 572. It should be noted that the concept of sovereignty was intended to be applied only to European, Christian states (later including North and Christianized Latin America), thus excluding state-like communities in Africa, Asia from benefiting from it. Furthermore, both Bodin and Hobbes lived during periods of intense clashes in the name of religion.

6 Nicolas Negroponte, *Being Digital* (New York: Knopf, 1995).

[7] Ian Angell, "The Real Politik of the Information Age," *Information Strategy* (January 1998).

[8] In many respects the hypotheses that have been postulated above mirror those that are fielded in the globalizations literature. The literature seems to be characterized by a similar continuum that ranges from the 'overt' thesis (the role of the nation-state in the international system has been fundamentally undermined) to the 'myth' type thesis (whereby globalization is exaggerated and nation-states have not lost their policy making autonomy).

[9] See, for instance, Gary King, Robert O. Keohane, and Sidney Verba, *Designing Social Inquiry* (Princeton, NJ: Princeton University Press, 1994).

[10] "Regulating the Internet," *The Economist* (June 10, 2000), 99-101.

[11] Gartner Group, "A Domain-Name Battle Puts Business with China at Risk," *The Monthly Research Review*, (March 17, 2001; June 10, 2001). Available @ http://www4.gartner.com/1_researchanalysis/0301mrr.pdf .

[12] Gartner Group, 17.

[13] There was an earlier similar high profile case in which a Bavaria Court prosecuted Compuserve executives in relation to anti-pornography rules.

[14] Jean Eaglesham, "Yahoo! Bans hate propaganda," *Financial Times* (January 3, 2001), 12.

[15] Jack Goldsmith, "Unilateral Regulation of the Internet: A Modest Defence," *European Journal of International Law* 11, 1 (2000): 135-148.

[16] Zak Muschovitch, "Taxation of Internet Commerce" (April 26, 1996; June 12, 2001). Available @ http://www.iprimus.ca/~zak/Taxation.html#note2.

[17] "International Taxes: Financial Services, Internet, Among Top Foreign Issues, Treasury Department Official Says," *Daily Tax Report* (Taxation, Budget and Accounting, January 19, 1996), The Bureau of National Affairs, Inc., quoted in Muschovitch, "Taxation of Internet Commerce."

[18] Karl Frieden and Michael Porter, "The Taxation of Cyberspace," *Cal-Tax Online* (December 1996; June 13, 2001). Available @ http://www.caltax.org/andersen/contents.htm.

[19] The OECD has a "Model Tax Convention" that is highly successful (almost 2000 conventions are based on this model), but the model is used to eliminate double tax imposition, and is not tailored for the specific needs of electronic commerce. See http://www.oecd.org/daf/fa/treaties/treaty.htm.

[20] Muschovitch, "Taxation of Internet Commerce."

[21] The Regulation of Investigatory Powers Act was passed into UK law on the 27th July 2000. It was a controversial bill that contains sweeping powers, which cover the interception of communications, intrusive surveillance, human intelligence sources, and the compulsory disclosure of encrypted data.

[22] Carnivore is a powerful computer program designed by the FBI to intercept Internet communications.

[23] In 1997, the G8 adopted a number of principles and a common action program against high tech crime.

[24] Further information on the OECD policy guidelines, for cryptography, privacy and security is available @ http://www.oecd.org/dsti/sti/it/secur/index.htm.

[25] Available @ http://conventions.coe.int/treaty/en/projets/cybercrime.htm.

[26] Comments of the Center for Democracy and Technology on the Council of Europe Draft "Convention on Cyber-crime" (Draft No. 25), Center for Democracy and Technology (CDT), February 6, 2001, June 29, 2001, available @ http://www.cdt.org/international/cybercrime/010206cdt.shtml

[27] See CDT, emphasis in the original.

[28] Comments from IP Worldwide available @ http://www.law.com.

GIAMPIERO GIACOMELLO has just completed his Ph.D. with the Department of Social and Political Science of the European University Institute with a dissertation on governments' control on the Internet, and is currently principal investigator on a project on "forgotten wars" with *Caritas Italiana*, Italy's most important NGO. Since 1996, he has been Visiting Professor of Political Science at the Center for European Studies of the Dickinson College, Bologna (Italy). His research interests cover research methodologies, computer networks and international relations. Giampiero Giacomello graduated (with a B.A. Hon) from the University of Padova and holds an M.A. in international relations from the Johns Hopkins University P.H. Nitze School of Advanced International Studies (SAIS). E-mail: giampiero.giacomello@iue.it.

FERNANDO MENDEZ is Ph.D. candidate with the Department of Social and Political Science of the European University Institute of Science. He holds a MSc. in European Politics from the London School of Economics and is conducting research on US and EU policy responses to cybercrime and e-commerce. E-mail: fernando.mendez@iue.it.