The Internet and the Future of Security:
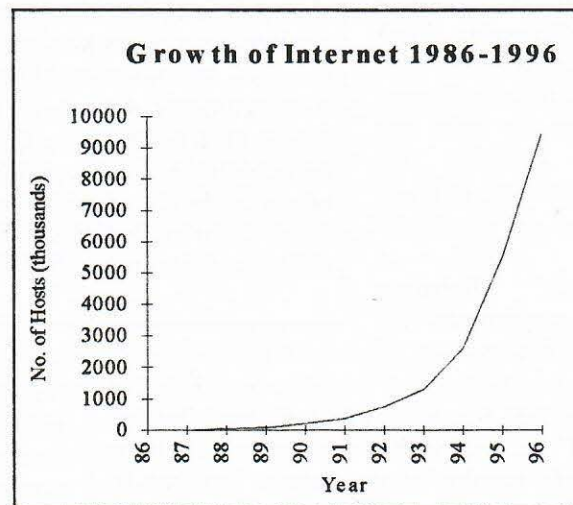## The Globalization of Space, Time and Image.
Erik Solem.

Introduction.

The Internet, which has been described – and quite correctly it seems – as an anarchic but liberating system, has grown at an explosive speed. By the beginning of 1996 some 9.5 million computers were directly connected to this global network, which is nearly a 200 % increase from last year. However, the number of users is, of course, even much larger. In addition to these 9.5 million computers, there are also machines which are jointly connected to networks with common access to the Internet. Since most of these machines are operated by several individuals, only a very rough estimate of actual users can be made. However, with, say, somewhere between 3 and 5 users per direct Internet access, this would give us an estimated figure of from nearly 29 million to 48 million users globally. IBM believes that by the year 2000 some 400–800 million users will be connected to the Internet.

The implications of this are staggering. For **International Relations**. some of the key questions are: What does this mean for such central concepts as Security and Foreign Policy Making? Will there be new forms of Warfare and Conflict Resolution, and if so what shape will these take? If previous notions of Censorship and Control are on the way out, as it seems they may be, what will – or should – take their

place? Or, is the question in fact redundant? This paper provides a conceptual framework and is a first go at some of these concerns.

Growth and Development of the Internet.

Growth of Internet 1986-1996

The growth and development of the Internet has been both quantitative and qualitative. According to Vint Cerf, it has gone from "near-invisibility" to "near ubiquity" in little

more than a year[1]. And if we look back somewhat further in time, the near explosive development of the Internet is evident. The above chart illustrates the system's quantitative success: As of January 1996 the Net's domain was more than twice as large as it was some six months before. Some 76000 systems were named **www**, up from only 17000 six months before. These are staggering statistics.

Not only in terms of sheer numbers and their implications, but also with respect to quantitative changes taking place **within** the user constellation of the Internet, some specific recent developments are worth taking into account. First, the **commercial** part of the Internet has now passed that of the **university** and **public** sector usage of the system. According to reports from Network Wizard, by the end of 1995 there were 2.4 million users directly connected to the Internet with the registration **com**, which in the U.S. signifies commercial services. This number represents an increase of some 45% compared to 1994. In comparison, the number of direct connections within the U.S. educational sector within the **same** period of time amounted to some 1.8 million, representing an increase of only 8%. Since U.S. trends in this domain, as well as in others, frequently signify larger, often global, trends, this observation is worth noting. A major implication of this trend is that we may now well be entering a **new period** in the Internet saga. If this is the case, no longer will "the Net" remain the domain of principally the computer literate and "net-initiated" aficionada. From now on it could in fact turn into the full-fledged open market place for trade and commerce, including the trade and exchange of ideas, as contained in its initial promise. And as International Relations theorists or practitioners this development should – and of course it does – concern us. Conflicting claims about the Internet such as that it is the "greatest free marketplace of ideas that has ever existed" and/or that the "most remarkable thing about it is the banality of the material that can be found on it" (Webb 1996), may now be observed more closely and tested. Although Keith Webb is no doubt

> The Internet is perhaps one of the most powerful agents of freedom of information that there is. Its informational ability to expose the truth to those who want it is nearly unmatched. And as long as we know that this tool, like many others, is double-edged, we should be on safe ground. What we must do, in this field of human activity as in others, is not to stop technology blindly, but to stop blind technology. The Internet, when understood and used properly could help us understand the difference and make the right choice.
> — Solem

right is stating that the truth, in all likelihood, lies somewhere in between these two opposing statements, we will no doubt from now on be treated to a different flavour with regard to the Internet, its usage and the perceived and *de facto* roles it will have in society in the near future.

Because of the quantitative and qualitative changes in the Internet's user constellation; because of the massive increase in usage, and because of the need for new services to stem the information overload, such new services will likely materialize. Tailor-made information packages and subscription services are already seeing the light of day. This process will increase and – only after a while– stabilize somewhat. The list of potential services on the Internet is almost limitless. Already, the entertainment industry is experimenting with ways of pumping movies and music through the Web directly into consumers' homes, bypassing a series of middle-men, such as retail stores or video-rental shops. It could, and will, also bypass various regulatory and/or controlling mechanisms. More about these later on.

The counter-argument to the above scenario ("rapid-growth/development") is the opinion among some observers that the Internet is merely a passing fad, which will fail because 1) it is incapable of keeping up with the growing traffic and 2) businesses cannot find a reliable method of selling their product over the network. It should be noted here that similar scepticism did greet the introduction of a whole host of other technologies, which are now taken for granted by almost everyone. And, all else being equal, the useful parts of new technology become embedded in our daily life.

Human history is full of miscalculations with respect to the introduction of new technology. The telephone and the car, for example, were at the time of their introduction, both denounced by critics as nothing more than "toys for the rich". The telephone and the radio were seen by some as the "destroyers of family life", and television was condemned outright by some observers. A no less reliable source than *The New York Times* reported after a prototype viewing of TV in 1939 that "the problem...is that people must sit and keep their eyes glued to a screen; the average American family hasn't time for it".

The problem we encounter here, therefore, is an age-old one. It is that people have always had, and will likely continue to have, a tendency to view new technology in terms of what already exists. To state about the Internet that it is "like TV" or "like a , only better" misses the point. To try and **define** it may even be an exercise in futility, as

---

[1] *"Computer Networking: Global Infrastructure for the 21st Century"* by Vinton G. Cerf, Senior Vice President, Data Services Division, MCI Telecommunications Corporation

the nature of the Web is both dynamic and unstable. We do not know what exactly it will evolve into. The only thing we do know, watching both quantitative and qualitative trends and changes, is the following: the present era, in which very large quantities of data of *every sort* can be replicated and transmitted at will, is going to create upheavals in how we work, learn, do business and interact with each other.

In the meantime the scramble is now on to try to meet a whole series of new services which the industry itself anticipates will be wanted. Already by later on in 1996, or early 1997, Compaq, IBM and other desk-top manufacturers plan on introducing low-cost Internet 'appliances', i.e. stripped down computers which can connect to a TV set and cost in the vicinity of $500 – or less. Other, more advanced systems, are on the horizon and they will meet (and change) many of the consumers' preferences and choices.

Security and Foreign-Policy Making.

Although security in the final analysis is more important than foreign policy making *per se*, the latter tends to take precedence in the ordering of the affairs of men. This, of course, may be a fallacy, but it has not deterred the foreign policy making establishments from making and acting on these assumptions. So let us first look at foreign policy making in the age of "the Net". Two, fairly brief, illustrations may suffice here.

Thomas Friedman of *The New York Times* reports an incident that caught his eye. A front page picture of the Financial Times shows Bill Gates, chairman of Microsoft, holding talks with Jiang Zemin, president of China, with a caption stating that the two men had held "very cordial" talks, in contrast to their "frosty summit" of 18 months ago. Friedman then observes that, this being the case, Mr. Gates will have met the Chinese President twice as often as the U.S. President Bill Clinton has within the same 18 month period. The journalist concludes – and he may be correct in his assumption – that "the Chinese believe they need Bill G. more than they need Bill C". He therefore poses the interesting, and for us quite relevant, question: "Does Microsoft have a foreign policy?" (Friedman 1996).

The direct answer to this question is that Microsoft does not have a foreign policy per se. But what the company has is a global business agenda. And since Microsoft today possesses twice the market value of General Motors it may well be, argues Friedman, that it would seem to be bound to influence U.S. foreign policy. But does it ? And does it have to? Microsoft is a $50 billion company, however, it has only

recently opened a Washington office. With an army of PR experts and lawyers to defend it against antitrust suits and copyright violations, it is unlikely that the company would need to look to Washington for any specific help. So, Friedman is right, Microsoft does not **need** Washington to open doors for it, since – it seems – foreign governments are more or less begging the company to enter their domains. And the general importance of China is due not only to the fact that the country has 1.2 billion inhabitants. It is also, as far as Microsoft is concerned, due to the equally important fact of China's restrictive birth control policies. With every family being restricted to one child, this means that there are often two sets of grandparents and two parents — a total of six adults – with the prospect of saving to buy a computer and software for each child.

Other countries which will be "up and running" in this process, as far as Microsoft is concerned, are Japan and Israel. The company's hottest market in the Middle East is Saudi Arabia. Does Microsoft, therefore, "influence" U.S. foreign policy? Is it, in fact, an "American" company? The answer to this last question, coming from Microsoft itself, is that it is a **global** company based in the U.S. Hence there is Microsoft Japan, Microsoft Italy...and so on (Friedman 1996). This does not mean, of course, that it is indifferent to the U.S., for the company needs a cutting-edge U.S. technology market to design, test and perfect its products prior to global market penetration. With a virtual world-wide monopoly, Microsoft operating systems run 85% of the world's computers, and give access to most, if not all, of the modern lanes of communications. The company resembles, in Friedman's words, one of the great sea powers of old.

Is what is good for Microsoft good for America? In one sense the answer is yes, and the explanation is as follows: In order to take advantage of the technology of which we speak, and which is desired by a whole host of recipient countries, societies have to be more open, deregulated and interactive. This is, by and large, good for democracy.

However, software technologies which make it possible for individuals to communicate horizontally across national boundaries through the Internet; which enable them to set up groups and information pools which are outside the controlling power of governments, **must** surely upset or frighten someone? one would think. And that someone is likely to be an individual or group of individuals "in authority". Apart from the general type of power-mongering found here and there, and the persistent desire in certain individuals for control over other people, there are in fact a few legitimate concerns. However, these tend in general to be related to crime and address themselves to quite specific issues, such as child pornography, which – at least until now – have been somewhat outside the confines of foreign policy making.

In the final analysis, it is difficult to predict what the full impact of "the Net" will be for the process of foreign policy

making. Chances are that, if understood and used properly it could provide great opportunities as an indispensable aid to decision making.

Turning to security, it is, perhaps, not all that easy to see that there should be some direct link between the operation of what has until now primarily been considered an information technology tool, (some sort of a super-library-cum TV with extras) on the one hand, and what one could conceive of as national or military security on the other hand. But consider the following news headline and subsequent story: "Logic bombs may soon replace more conventional munitions" (Economist 1996). This article, based on a scenario development from the U.S. Pentagon military planners, may well be of particular interest for future International Relations theory and practice. In this scenario (future history) several local computer users, when trying to log on to the global communications network, find it impossible to connect. In horror they watch their computer hard-drives becoming clogged with streams of incomprehensible e-mail messages containing tens of thousands of lines at a time. Concurrently, managers of large www. (World Wide Web) information sites watch helplessly while their large server computers hopelessly grind to a halt after being overwhelmed by tens of thousands of simultaneous requests for data. It is several hours later that engineers at telephone companies, defence labs and universities start to realize that the streams of data traffic swamping the Internet connections are in fact in no way accidentally caused. Rather, according to this scenario, they originate from **outside** U.S. territorial grounds. One clue is the way that the packets of data flooding the network keep changing their addresses of origin, they seem – in this story – to originate somewhere in Eastern Europe.

A few days later, the lights have gone out, telephone lines are jammed solid, trading on the New York Stock Exchange has stopped, automated teller machines have started indiscriminately crediting and debiting customers' accounts, airlines have lost their air-traffic controls, and the ghastly realization dawns, America is under attack, the victim of a cyber war (Economist 1996).

This is of course fiction, but such scenarios are now being developed in the U.S. and in defence departments elsewhere, as well as (one should perhaps hope) defence science labs. According to at least one Silicon Valley technology guru (Geoffrey Baehr) it is quite clear that, by now, a network war could halt a country's economy as effectively as an electromagnetic pulse would following a nuclear detonation. Several similar scenarios have been developed by, for example, researchers at the Rand Corporation. Some

of these, assuming they become unclassified, may be available to International Relations. experts in the university world in the near future.

Scenarios and strategic games are now being drawn up, and it seems certain that the question of "information warfare" is taken seriously by top military brass in many countries. Roger Molander of the Rand Corporation's Washington office, for example, has developed several such security-related exercises. They have tended to raise as many questions as answers, but at the very least these "serious games" have alerted military and strategic planners alike to some of the information based security threats in the future.

We may now have to understand "security" as a much broader concept than that traditionally applied by national defence planners. Security is closely related to strategy, previously a somewhat narrowly defined concept. Until fairly recently in many circles the concept has tended to be based primarily upon military power per se. We will therefore propose an alternate working definition for present purposes. It seems to us that for very good reasons a strictly speaking "military strategy" for a nation is no longer sufficient, if indeed possible. In many instances, for example, the line of demarcation between military, economic and political matters is no longer clear-cut. Hence, the development of a long-term strategy for national survival, even with its military meaning intact, will of neccessity have to incorporate political, economic and even social factors. Conversely, political strategy is by now increasingly seen as firmly based upon military and economic power realities. Does foreign policy making, then, base itself upon or does it determine security? To arrive at this point of conceptual **agreement** with subsequent prescription for action, a fair bit of work has to be done, in most Western countries, at any rate.

As we have seen, the state is no longer the only actor in International Relations. But to the degree that it remains the primary actor and guarantor of national security, the following major assumptions ought to be kept firmly in mind. For security to be achieved, strategy as applied here, must be seen in its broadest terms. As such it amounts to the art and science of employing all elements of power of a nation to accomplish the objectives needed in **peace** or war, and – increasingly – within so-called "peace crises". Strategy in this sense, therefore, involves the use and close integration of the economic, political, cultural, social, psychological, moral, and even spiritual power available. According to this line of thought, strategy can be formulated only after the objectives to be accomplished have been determined. Hence national objectives and national power are irreducible elements of national strategy. When national objectives have been determined, all aspects of the **problems** confronting the nation should ideally be thoroughly examined, and accurate evaluations made of the character, size and capabilities of the various elements of national power available for the construction of an optimum

strategy. This type of strategy, then, should be flexible enough to counter unexpected moves by any adversary, hence strategic options – or contingency plans – are necessary ingredients in the overall scheme (Solem 1986)

If this sounds like a good counter-conventional scheme for meeting some of the challenges of the future, such as they present themselves for purposes of proper foreign policy making or for the maintenance of national security, it probably is. And will new forms of technological informational and analytical tools based on the bridging of gaps and on technology break-throughs – such as the Net – help us in the construction of such a scheme? The answer would seem to be an unqualified yes.

Censorship and Control.

We had stated at the outset that perhaps some of the previous notions of "censorship" and "control" were outdated, and that a remaining question might be: what would – or should – take their place? As a corollary, is that question itself redundant? According to the present Norwegian Prime Minister, Mrs. Gro Harlem Brundtland, new technology will demand new forms of co-operation among countries. Censorship and control, in the context of the information society, which is the direction in which we are now collectively steering – for that reason alone – becomes impossible. The informational – and bio-technological – revolutions, within which it seems we now find ourselves, possess such characteristics that, according to Mrs. Brundtland, the "boundaries of censorship are being exploded". This claim seems to be a fairly visionary, perhaps even revolutionary but essentially correct way of viewing these developments. Attempts by individual countries to use national legislation in order to suppress the content of the net are bound to failure, according to the Norwegian Prime Minister. Instead of applying such traditional methods as censorship, control and regulation, work should be undertaken to try to influence attitudes. International co-operation, therefore, becomes important and takes on renewed relevance. Furthermore, since the private sector seems to be ahead in the game, the public sector ought to follow suit.

Information technology (IT), in which the Internet becomes the central component will doubtless create new lines of demarcations and perhaps even new classes of people. The old, very unattractively sounding concept of "gods vs clods", which was bandied about a decade or so ago, could take on a new relevance. One may hope that this will not be the case. The scenario of a world consisting of those who control and can operate the technology in question *vs*

those without knowledge and access is far from pleasant. It seems in some way offensive to the egalitarian element of the human spirit. Should, therefore, the notion of full and equal access to and development of I.T. be made the principal goal of action in this arena? Consider some related important and possibly intervening trends. Within the year 2000 one half of the poor population of the world's less developed countries (LDC) will live in cities. Increasingly, rural populations decrease – due to lack of employment opportunities – whereas the urban populations increase. By the early part of the next century the number of mega-cities (more than ten million inhabitants) will rise sharply. Mexico – by now the world's largest city – is soon approaching 25 million inhabitants, followed by São Paulo, Brazil, with 22 million. Calcutta, India has nearly 16 million whereas Shanghai, China and Bombay, India have populations of 15 million. According to recent United Nations statistics, whereas there were 1.4 billion city dwellers in 1970, that figure had increased to 2.4 billion in 1990 and- by the year 2000 will have reached 3.2 billion. Further out, according to the U.N. and calculations, the urban populations could reach 5.5 billion by the year 2025.

Add to this the rather deplorable conditions under which these individuals try to eke out their existence. Some 300 million, which is nearly a quarter of all LDC city dwellers, live under what the U.N. describes as life-threatening conditions and extreme poverty. The lack of water, absence of proper renovation, massive pollution, very high unemployment and an increasing level of homelessness will contribute to make this situation more dangerous, perhaps even explosive.

Information, education and the development of democracy by itself may not be the panacea for salvation. But anything that tries to stop or in some way stultify mankind's knowledge of what is actually going on seems to us to be a step in the wrong direction. For that reason alone, the attempt to try to limit or restrict the content and/or use of the Internet would probably not succeed, nor should it. This does of course not mean an absence of some sort of user's code of ethics, which is an entirely different thing. We know of misuses and misapplications of the Internet, such as harassment cases, or stalking, but these appear in other avenues of life also. And, needless to say, the important legal task ahead with the Internet is less the writing of new laws than the working out of proper parallels and analogies between Internet acts and real ones.

Real security lies in the protection of human rights and in our ability to freely develop ourselves without undue constraint or real danger to others. This, of course, brings us in a sense full circle back to some very important and basic normative questions. To quote Vinton Cerf: "Truth is a powerful solvent". The Internet is perhaps one of the most powerful agents of freedom of information that there is. Its informational ability to expose the truth to those who want is nearly unmatched. And as long as we **know** that

this tool, like many others is a two-edged sword, we should be on safe ground. What we must do, in this field of human activity as in others, is not to stop technology blindly, but to stop blind technology. The Internet, when understood and used properly could help us understand the difference and make the right choice.

A COPY OF THESE *PROCEEDINGS* HAS BEEN SENT TO CLUB OF ROME ASSOCIATIONS IN THE FOLLOWING COUNTRIES:

ARGENTINA - AUSTRALIA - AUSTRIA - BULGARIA - CHILE - COLOMBIA - CROATIA
CZECH REPUBLIC - EGYPT - FINLAND FRANCE - GEORGIA - GERMANY
GREAT BRITAIN - HUNGARY - ITALY - MEXICO - THE NETHERLANDS
NEW ZEALAND - POLAND PUERTO RICO - RUMANIA
RUSSIA - SLOVENIA - SPAIN - UKRAINE - USA - VENEZUELA

AND TO THE PRESIDENT AND SECRETARIAT OF THE CLUB OF ROME

Erratum

We regret that there was an error in the eighth row of the right-hand column of the Table at the end of Prof. Jerzy A. Wojciechowski's paper "Knowledge, Environment and Ethics" in the March 1996 Proceedings. The complete Table is reprinted below with the correction highlighted.

Differences in Perception of the Earth System

Nature is:	Infinite i.e. Inexhaustible.	Finite: i.e. Exhaustible.
Hence:	No exploitation of nature.	Exploitation of nature.
	No negative effects for: a) nature. b) humans	Negative effects for: a) nature, b) humans.
	No responsibility for exploitation of nature	Responsibility for exploitation of nature
	No responsibility for the development of powerful knowledge.	Responsibility for the development of powerful knowledge.
	Does not threaten nature.	Threatens nature.
	No humans/nature moral problem: no need to enlarge the moral problematique.	Moral problem: humans/nature: need to enlarge the moral problematique.
	Scientific (quantitative) knowledge sufficient: no need to complement it by enlarged knowledge of qualities and values: humans may imagine themselves as masters of the world	Scientific (quantitative) knowledge insufficient: need to complement it by enlarged knowledge of qualities and values: **humans are not masters of the world**.
	No source of concern about its effects on nature	Concern about its effects on nature.
	Ethics is secondary.	Ethics is primary.