The Ironies of Information Technology: The opportunities and pitfalls of Information Technology for Human Rights

By Shayne Weyker
University of Maryland College Park
Department of Government and Politics
weyker@wam.umd.edu

Presented at the Conference on Globalization and Human Rights
Irvine, California
January 15-16, 2000
Revised: 4/18/2000

Introduction

There has been a small but extremely interesting literature on the role new information technologies [1] have played in aiding such values as human rights, democratization, and economic justice.[2] But the literature has been somewhat lacking in generalization of particular examples into larger trends. This paper will attempt to fill that gap, while giving a wide overview of the technologies involved. It begins in part one with an explanation of what social movements do and why advances in information technology have great impact on their work. Part two continues with discussion of how information technology is empowering the human rights movement. Part three concludes the paper with a discussion of the various ways the promise of technology may be neutralized or turned against human rights workers.

In this article human rights organizations will be conceived of as entities which are constantly trying to (re-)organize themselves as well as receive and transmit information for the purpose of reacting to and modifying their environment. Thus the opportunities and pitfalls of technology will therefore be discussed in terms of their effects on human rights organizations as self-organizing (cybernetic) entities.[3]

Part I: Why Does Information Technology Matter?

The short answer is that it matters because information lies at the heart of what Non-Governmental Organizations (hereafter NGOs) do. If technological advances allow them to do these things better, the movements and organizations become more capable and thus, all else being equal, more effective and powerful. For other technological advances that hinder their ability to do their job or provide a relatively greater advantage to their opponents, the opposite would be true. Back in 1982, a few years before camcorders, faxes, desktop computers and the internet became part of many people's lives, a scholar on NGO's wrote:

> [NGO] personnel, particularly at the leadership level, become professionals in the use of information. Generally, . . . [groups promoting a position] have very limited financial resources . . . [or] ability to apply physical coercion [even terrorist violence is political rather than military in nature] . . . The ability of NGOs to apply pressure is through the mobilization of legitimacy for their cause. Winning support by changing people's perception of the issues is done by presenting arguments and information . . . [NGOs] must find and transmit relevant information and once such propositions are established [as true in the minds of target audiences] they have to continue to provide information which reinforces propositions. . . . Processing of information is always a major activity of pressure groups and often it is overwhelmingly the most important activity.[4]

But, as he notes, this information must be perceived as invariably objective and truthful or it will be ignored. This is because social movements lack the reputation that states do for having accurate and complete information. Moreover, they lack the coercive and legal power of states. Thus, movements' pronouncements do not carry weight simply because of who says them. He continues, In this unequal contest pressure groups cannot afford to make mistakes because thereafter their statements will not so readily be given credibility and references to mistakes will be continually thrown back at them. . . . After some time many pressure groups do get accepted as trustworthy . . . this can

give them privileged access to governments [tremendously increasing the group's influence, but only as long as the trust is maintained].[5]

So well-researched, professionally-presented, truthful and factual information, turned out quickly enough that it can be passed to the right people at the right time, is what makes produces results for social movements. One could put it more abstractly by saying that movements depend on quickly and accurately doing five things.

1) Collecting information from the environment.
2) Processing that information.
3) Making internal changes based on that acquired information, where such changes are helpful.
4) Preventing harmful internal changes.
5) Sending information back out to (certain people in) the environment which will cause changes in that environment.

These things in turn imply the need for capabilities such as; foresight, preventing "oversteering" (over-reacting), minimizing lag times, minimizing noise that obscures the information/signal the group wants to send, and expanding the size of the audience that can be reached by the group's message.

Brysk offers an updated view of what social movements do and how they do it, particularly in regards to Latin America.

> The state can be transformed from above and below because it may control territory, force, and resources, but it cannot monopolize information and legitimacy. . . . [social movements gain power] by projecting cognitive and affective information to form international alliances.[6]

Note the distinction Brysk makes between cognitive information and affective information (which are defined below). Participants in movements try to influence those in power by tapping into the potential power of bystander reference groups in other countries to achieve several benefits to their cause. These involve the reference group:

- supporting the movement (assisting information gathering, processing, and distribution)
- applying pressure to the government the movement operates under via direct means (making the environment for the organization more hospitable as well as amplifying messages sent by the organization to particular persons with power), or
- applying indirect pressure by lobbying their own government to apply such pressure.

Brysk believes that the Argentine human rights movement, for example, and many others like it:

1) have an informal division of labor between producing "political theater" (affective information which elicits an emotional response) to raise public awareness and producing "documentation" (cognitive information which gives an understanding of the extent, details, and mechanics of the problem) which is needed for international policy decisions.[7]
2) "achieve their impact through persuasion--the use of information to change behavior and institutions through changing perceptions and values".
3) "use and contest factual information to reach international publics and challenge (domestic and international) institutions"
4) "project patterned symbolic information as images that mobilize legitimacy for the movement"
5) are helped if there is "recognized a legitimate international concern by international laws, treaties, and organizations that provide a point of entry to transnational alliances" which the conception of sovereignty is not considered to be applicable against.[8]

Before going on to discuss examples of how information technology can be helpful, it is useful to quickly consider the idea that in some ways information technology is fundamentally ambiguous,

perhaps even conflicted, in its relationship to the work of human rights organizations. As Rosenau says,

> Throughout the world today . . . the sources of authority have shifted from traditional to performance criteria of legitimacy. As a result, structures of authority have entered a period [of] crisis, with the readiness of individuals to comply with governing directives being very much a function of their assessment of the performance of the authorities [at meeting goals, satisfying needs, and providing stability].[9]

Put another way, governments find themselves faced with the problems of;
1) Noise and hostile messages feeding-back upon themselves and undermining the government's ability to communicate messages which build legitimacy (a friendly environment) for itself.
2) The government having to act and produce results faster than before (leading to greater risk of oversteering, insufficient foresight to act in time, and acting without a coherent plan).
3) A trend towards (what to the government's leaders is) an undesirable internal reorganization of society.

Rosenau writes about how this empowers sub- and supra-national actors as people decide that such actors can perform better for them, leading, presumably, to people shifting their allegiances.[10] But there is also the possibility that the more demanding and more analytically competent constituencies may be more difficult to keep organized and moving towards a common goal when times are hard and progress is painfully slow despite the obvious importance of unity. That states suffer from this legitimacy crisis is the very reason NGOs can build the support they do. But NGOs may have to face this problem as well. Information technology can provide increased speed as time required for gathering, processing, and distributing information is cut. But the speed "arms race" complicates all organizations' efforts to avoid over-reacting and other making other kinds of errors while acting fast enough to stay ahead of what rivals are doing. More contradictions like these will appear as the same technologies and sometimes even the very same effects created by their use appear as both beneficial and dangerous to human rights NGOs.[11]

Part II: Technology To The Rescue

The first of the real strengths for information technology use by human rights organizations is that computers improve the ability to marshal the facts (cognitive information) on their side into a very persuasive logical argument. Information technology speeds up, enlarges the scale, and improves the quality of information collection and processing by human rights organizations..

Dan Salcedo, then Human Rights Coordinator for the American Association for the Advancement of Science,[12] recounted an interesting example of this from El Salvador, where human rights groups associated with the Truth Commission were trying to find out who was responsible for human rights violations by the government, so that these people could be removed from power. The human rights groups were able to acquire two separate sets of data which separately are of little use for that purpose. One, a "military map", showed which military officers were in command in which regions of the country at which times. The other was a long list of confirmed human rights abuses that included, of course, when and where the abuses took place. Both of these sets of data were combined in a computer database and the computer was then asked questions such as: 'Which officers, of those still in service, have accumulated the greatest number of human rights abuses in their jurisdiction while they were first or second in command?'. This produced a list of officers who were then removed from the military based on this highly credible evidence that they either ordered abuses or allowed abuses to occur by their subordinates on a continuing basis.[13]

The next generation of such projects by human rights groups will likely involve the use of Geographic Information Systems (GIS), geographic databases that link data to elements of a computer generated map. This produces information-rich, easily redefined, maps that can let a person viewing the map quickly and easily see where the greatest intensity of abuse is taking place based on hard data rather than have to wade through many charts and tables or trust someone else's general conclusions. This would reduce the lag time and noise associated with policymakers trying to understand and verify the full extent of the claims made by human rights advocates. It is also worth noting here that the United States' new willingness (seen in Kosovo) to use its high-resolution satellite reconnaissance capability to expose recently dug mass graves could be useful in quickly resolving disputes among countries about whether or not there are massacres of civilians taking place.[14] While having solid objective (cognitive) information does not guarantee policies more favorable to the protection of human rights will be enacted, it is very likely helpful.[15]

The other main type of opportunity technology offers for human rights lies in telecommunications and computer networking technology, particularly the advent of the globe-spanning internet. These allow the creation of massive "network organizations" made up of hundreds of small organizations pooling their information and possibly their labor. This can greatly multiply each participant's access to information and ability to coordinate. Even better, people can do so without having to actually combine to form one single huge organization, with all the sacrifices that implies. A classic example of such information sharing and coordination was the Zapatistas' effort to win a public hearing of their grievances during their uprising in Mexico. This advent of this kind of network organization has several important effects.

First, the availability of new communications technology offers a better capability to draw other people into a human rights group's organizing efforts. New communications technology also allow activists to share their own experiences, information, tactics, etc. as easily as if they lived in the same country.[16] Consider the following example from the Mexican labor advocacy group Mujer a Mujer:

> "For our first six years [1984-1990] we depended on 'border trips': every two months, two of our members would travel 24 hours by bus to a friend's house on the U.S. side of the border, where we would take turns in a marathon of long distance calls--to organize events and keep in touch with key contacts. Now [thanks to computer networking] we are in daily coordination with our key contacts throughout the region."[17]

Second, news of crises can be spread instantly to unlimited numbers of interested people who want to help. A huge surge of moral (affective) or technical (cognitive) support for those calling for help as well as condemnation for their enemies creates opportunities for a global on-line cathexis (spontaneous collective action). An example of cathexis (or at least an extremely fast organized response) occurred when the Chinese government ran pictures of democracy protesters on TV and asked for tips on their location so they could be arrested. Thousands of bogus phone calls immediately flooded in from across the globe to overwhelm the government's information-gathering effort with noise. Another, somewhat more structured response, in response to a severe attack by neo-Nazis on foreigners in a German city, was sending thousands of faxes denouncing the attack to that city's local newspaper in less than 24 hours.[18]

The Internet also shifts activists' access to media, as seen in the Zapatista's case. Reactions to articles written about the conflict on the internet appeared with little or no delay and without the filtering of editorial page editors deciding which letters would see print and which would not. Beyond this, interacting through the internet allowed activists to see their own protests against the Mexican

government's actions as part of a larger movement, because they were able to read others' eyewitness accounts of protest actions. Also, on the internet reporters from small newspapers and activist groups received just as much attention as reporters from major newspapers. This strengthening of opposition voices relative to establishment ones was important. Reading other like-minded people's analysis and debate provided readers with a sense of collective concern necessary for taking committed forms of action.[19]

Such networks have become tools for undermining government censorship, due to their resilience, wide accessibility, and frequent underestimation of the importance of such networks by governments. Thus the state's power of coercion to shut down NGOs' attacks on the government's legitimacy can be neutralized with the right combination of tools, skills, and courage.[20] For example, the Zapatistas evaded censorship by the Mexican government despite its control over the mass media in that country. Individuals sent reports out to usenet newsgroups, PeaceNet conferences, internet mailing lists, and potentially sympathetic groups of people. Frequently, messages were forwarded by recipients. Forwarders would sometimes include translations from Spanish into other languages as well.[21]

To summarize, computers have helped human rights NGOs to create impressive new kinds of hard (cognitive) information. Camcorders put the power to create powerful affective symbolic imagery into the hands of anyone with something symbolic to record, such as the famous image of a Chinese man blocking a column of tanks. Computer and fax communications networks allow for the creation of dialogue and planning of joint strategy across long distances at low cost. Those same technologies allow movements operating under hostile governments the ability to contact and mobilize a large number of people fairly quickly. Electronic communication networks also allow direct application of public opinion pressure by those tied into the network without regard for geography.

The opportunities of technology for human rights groups are only half the story, however. We now move on to a consideration of the dangers posed by technology.

III: Pitfalls of a Wired World for Progressive Social Movements:

Several problems are discussed below that have to be avoided in world of extensive communications and information processing if the promise information technology holds for human rights is going to be realized rather than neutralized or subverted.

The First Pitfall: The proliferation of voices and the problem of "noise"

One particularly relevant feature of social movements is their susceptibility to being harmed by "subgroupism" or internal division.[22] This is characterized by a lack of consensus on what the proper objectives are and what means should be used to achieve the group's ends. While groups must be sufficiently democratic that the membership feels they have a fair share of control, such a lack of cooperation can prevent the sufficiently quick and accurate execution of some or all the five key informational tasks an organization must carry out to be effective.

> The lack of a strong bureaucratic structure for most groups and the fact that they are voluntary associations means that there is no central authority. There will usually be some central decisionmaking body, but it has little ability to enforce decisions. So the leadership . . . has to try and maintain a consensus within the group. Breakdown in the consensus can be more damaging to [groups promoting a cause] . . . than to other groups [(companies, unions, governments)] . . . which have economic interests to help hold them together.[23]

The enabling of more 'ground-level' members of the human rights movement in the countries where rights violations are occurring to communicate directly and instantly with the outside world without working through the movement's hierarchy can potentially damage the human rights organizations' precious credibility. These 'ground-level' people could speak using an international NGO's name to the media or reference public and unknowingly make false statements because they failed to do the necessary verification. Even if these people are correct, there may be a zero-sum game involved between the rank-and-file and the organization's headquarters for the attention of the reference group and journalists.

Breyman argues that decentralizing authority in NGOs would be a good thing.[24] But advocates of centralization would argue that losing the filtering mechanism that comes with concentration of the power to release information to the world may create counterproductive 'noise' in the organization's information channel to its reference public and the media. This could take the form of different statements contradicting one another, a glut of calls for action, unpredictable spacing in time of calls for action, and so on. Too many calls for action could alienate the press and demoralize reference group members. And conflicting statements could damage the group's credibility.

Organizational discipline and strong legitimacy of leaders and professional staff with those in the field might resolve the noise problem. But strong discipline and popular leadership are not always an easy combination, especially for a volunteer organization people can opt out of. Remember Willetts' observation above that volunteer organizations without an economic self-interest for its members to stick together and compromise are highly vulnerable to dissent and division.

The proliferation of information technology may intensify an already existing tension, between those in a movement who want rapid response and maximal results on the current case against those (usually higher up in the organization) who are more interested in protecting the movement's long term capabilities. Amnesty International USA (hereafter referred to as "AI") has a newsletter called Freedom Writers that it distributes. The newsletter contains sample letters which the reader can draw upon to write their own letters on behalf of people whose rights are being violated. Several years ago, a woman named Caryn Graves began to be distribute the newsletter in electronic form, typing them in to her computer and posting them to a the soc.rights.human usenet newsgroup read by thousands of people, including some critics of the human rights movement.

AI asked Ms. Graves to stop doing this. They were concerned with such a broad distribution of their message in an electronic text form, because electronic text is too easy and inexpensive to modify and redistribute. Eventually people might begin receiving forwarded copies of these messages with non-Amnesty material added in by the forwarding person, but with Amnesty's name still in the message. It would even be possible to create a fake issue of the Freedom Writers newsletter, one appearing genuine to the casual reader. Since malicious messages with false claims of AI authorship had appeared on the internet before, AI felt that the instruction included in the newsletter to not modify it or redistribute it electronically would not be adequate protection against the above two dangers. Nor is this problem unique to AI, at least one individual human rights advocate once found some "bizarre and damaging" articles falsely posted under his name on the internet.[25] And Human Rights Watch has had faxes falsely sent out under its name in India.[26] To this day the newsletter is only distributed by email mailing list and via the AIUSA web page at http://www.amnestyusa.org/group/aicasework/fw.html.[27]

Subsequently, Ms. Graves had begun to distribute the Freedom Writers newsletter via an email mailing list with Amnesty's approval. Internet users can subscribe to such a list and have the newsletters sent directly to them via email. This email mailing list was unmoderated, meaning anyone could send messages that all subscribers would receive. On March 30th, 1998, someone other than Ms. Graves posted a message to the Freedom Writers mailing list, a message that seems to have

originally been written by a group called the Asian Students Association. The message was a call for action regarding someone named Andi Arief, who had been kidnapped at gunpoint. In the message readers are told about him and some others and asked to petition the Indonesian government for his and the others' release. This message was not created or approved by Amnesty. So readers had no way of knowing whether Mr. Arief or the others would qualify as a prisoner of conscience and whether the circumstances of Mr. Arief's capture had been verified to the extent Amnesty verifies such things before making calls for action.

This problem of "noise" when more people gain access to the channels of communication, which are used to speak to a human rights group's supporters, may have its origin in a related problem. Informational bottlenecks can occur in the human rights organization, making the increased information processing capability gained in other areas useless until the bottleneck in a particular problem area is cleared. In the area of human rights for instance, there are (even for the largest organizations having significant human resources around the world) many more cases of rights abuse being reported by the movement's rank-and-file than can be verified and then given sufficient publicity and international attention.[28]

Patrick Ball and his co-authors said something that suggests why there have not been more such attempts when the above theory suggests more should occur. Ball and his co-authors said that even as human rights groups in the developing world acquire more tools which can be used to communicate calls for action to potentially sympathetic people around the world, it does not follow that such groups will do so merely because they can. Many human rights groups operating in oppressive countries make it their business to carefully document and analyze patterns in rights violations so as to preserve the truth and identify abusers for the record rather than try to bring individual rights violations to the world's attention. For these groups to publicize rights violations and conduct international calls for action would have two negative effects on them. It would distract the groups from their original mandate and aggravate the danger of reprisal to their members. So such groups leave it up to others like Amnesty and Human Rights Watch to do such things.[29]

Clifford Bob offers another reason for why there is not a problem with front-line and top-level human rights workers competing for the public's attention. While he is primarily interested in how groups with human rights grievances attract the support of international NGOs, some of his analysis applies to attempts to gain the support of reporters who cover human rights stories as well. He suggests that a group seeking international support is better able to do so if it possesses certain qualities. Here are some of the qualities he believes are important.

- the ability to present their case abroad
- knowledge of the developed world
- skill in a major world language
- pre-existing contacts with people in the press
- the extent to which the group's goals are universal rather than parochial[30]

Given this list it should be easy to see why reporters for major newspapers and television networks in the developed would be more inclined to act upon information given them by the international NGOs than individuals or local groups. International NGOs professional staff have all of the above qualities, while oppressed groups in developing countries will typically only have only some of them. So while we may have reason to believe that people in developing countries are technically gaining the capability to communicate directly with the global press rather than through international human rights NGOs, reporters are just more predisposed to listen to the international NGOs.

There is mixed evidence on the extent to which the proliferation of voices and the concomitant problem of noise present a danger to human rights organizations. But such organizations should be aware of the problem and design their communication strategy to overcome it.

The Second Pitfall: Unfavorable environments for using technology to aid human rights work

The complimentary social organization (infrastructure) required to effectively exploit the new information that becomes available with the spread of technology is sometimes lacking.[31] Lipschutz notes that besides the technology, it is just as important to have, at least for people who want change, "new ways of doing things, of acting, of engaging in political and other activities." If the information produced lacks context (and is thus misleading/confusing), or is shaped by market forces, or is susceptible to the political agendas of media-owning capitalists, or is overly influenced by government 'news management', then its utility for progressive political purposes is reduced.[32]

Lipschutz's criticism seems to be most valuable for re-evaluating those communication technologies which must ultimately depend on the commercial mass media for their full effect. Heavily organized large demonstrations that are not covered by the press would be a stereotypical example of this. To what extent the human rights movement's efforts will continue to depend on the cooperation of commercial mass media may be an open question however.

Moving to the global level again, it is interesting how Lipschutz's criticism confirms Brysk's observation that having a structural "point of entry" into the international regime of international law and standards of behavior is very important to a movement's effectiveness. If the international legal and media opinion 'context' both in terms of reaching foreign publics and foreign elites is unfavorable to the movement's cause (lacks a "point of entry"), then NGOs' persuasive efforts have more difficulty.[33] For an exploration of how this works in practice, refer to the article by Clifford Bob.[34]

Additionally, at the domestic level, there has to be a "point of entry" as well. People have to some extent to be psychologically ready to hear the message from the channel its going to come to them on. Oscar Landi[35] notes that there was an intense cynicism and tendency of the people to disbelieve the post-dictatorship Argentine press when new discoveries of the old regime's outrages was publicized for the first time. This was because of the media's reputation for lying to aid the government in power and truth-obscuring sensationalism. To use another example from the domestic level, Ronfeldt points out that long before the Zapatistas' uprising in Chiapas, there were both relatively more than average international contacts (with Central American guerillas, arms dealers, and drug smugglers) and more regular contacts between NGOs and the people there. That, he says is one important reason why the uprising started there and not Guererro or Oaxaca.[36]

Second, there is another kind of domestic infrastructure, a legal one. Annis notes that, at the time of his article, the military in northern Guatemala was hostile to the proliferation of two-way shortwave ('ham') radios and controls their possession tightly. They army likely did this more out of fear of the military usefulness of such radios in the hands of rebels rather than a desire to crush free communication in the region.[37] In general, governments involved in a serious ongoing internal conflict that come to believe that the spread of a given technology (including things such as two-way radios, cryptography, and satellite maps of the country's territory) helps their enemies may tightly control and regulate that technology. Technologies the government believes are vital to economic growth might be an exception. But sometimes a government fearful of the free flow of information purposefully tries to hinder the free flow of information, even when that information is used for peaceful means.

One way of purposefully hindering the flow of information is to imprison the people who contribute to it. An example of this can be seen in the Chinese government's giving a two year prison sentence to someone accused of selling a list of 30,000 email addresses in China to a dissident internet news service. That service, VIP Reference News (also known as Dacankao) reprints articles about China from major publications not available to most Chinese and emails them out to Chinese residents. More recently the Chinese government arrested a citizen with dissident contacts in Hong

Kong who was preparing to publish a political book on the internet. He was charged under a law prohibiting communication with foreigners.[38]

Human rights organizations looking to use technology need to do three things here. First, do not attempt to communicate with (or through) people disinterested in the organization's cause. Also, avoid communicating on a channel audiences distrust. Second, plan around the presence or lack of extensive face-to-face contacts between the organization and the local people. Finally, plan around any laws that prohibit full and open use of communication technology.

The third pitfall: New vulnerability to sabotage and surveillance

A reliance on sophisticated communication technologies such as e-mail networks and the telephone/fax creates the risk of government wiretappers intercepting sensitive conversations, e-mail, and data which can reveal identities of members and group plans on a continuing basis.[39] The same databases that make it possible to carefully document patterns of human rights violations are themselves vulnerable to being copied by the authorities without the human rights organization knowing about it.[40] The advent of worldwide availability of very powerful and free encryption software (Pretty Good Privacy or PGP) to help prevent the interception of e-mail and other data reduces this threat, but does not eliminate it.[41] It is worth noting however that PGP is used far more often to protect stored data than to protect email conversations. Because of exhaustion with resisting constant government surveillance and their low level of computer skill, many human rights workers in developing countries resist consistently carrying out the necessary extra work to use PGP with email.[42] Some human rights workers who are uncomfortable with the added work of PGP are turning to the easier to use web-based encrypted email service HushMail that automates the encryption and decryption process more effectively.[43] HushMail does require a relatively stable connection to the internet however, something not all human rights organizations in developing countries have.

Also, according to security expert Carl Ellison, web-based encryption systems are vulnerable to being compromised by attacks where the user's connection to HushMail is redirected a different web site on the internet owned by the authorities that impersonates hushmail.com and lets the user type in their message. Ellison believes this is just one of a new wave of threats to private communication based on electronic impersonation. Now that it has gotten so hard, with strong encryption being used, to eavesdrop on the communication of others, it is simpler to pretend to be the intended recipient of the message.[44]

However, the safety of witnesses to rights violations who are identified in PGP encrypted documents would often depend on not on secure email , but the security of the encrypted document file identifying witnesses and the key to decode it staying out of the wrong hands. In one recent case a human rights observer was arrested by the government in Kinshasa with the names of witnesses encrypted in a file on his computer. Fortunately, he resisted coercion to give up access to his secret code key until his release could be obtained. Another such researcher with encrypted data on witnesses in Kosovo had his computer confiscated from him.[45] Several other layers of security can be and are used to control access to such sensitive information however.[46] In any event, as one human rights worker points out, sensitive human rights information about witnesses or the organization's tactical plans do not really have to remain secret very long. The secrets need only stay secret until the organization releases its report after witnesses have testified (or prepared against reprisals), or until the NGO holds its planned demonstration.[47]

Separate from the issues of interception, there is also the possibility of government sabotage of computers and phone lines. This was considered a real enough threat by the democracy movement doing vote counting in 1988 Chile that it felt the need to have a redundant fax-based vote reporting

system simultaneously with a much more efficient (but vulnerable to sabotage) computer based one.[48] Amnesty International recently had problems with the Tunisian government not only intercepting but also interfering with the delivery of the local section's email.[49]

Another way governments can attempt to sabotage Human Rights groups ability to distribute or receive information is by blocking its own residents' access to web pages on the internet containing content the government disapproves of. This is currently done in places like China where the government controls the high capacity connections (called backbones) that most data must pass through to get into or out of the country. But while site blocking may stop the casual web surfer, people who really want to find such information will locate what are called proxy web servers which provide the content of blocked web pages on an unblocked web page, thus bypassing the block. When access to a proxy server is blocked, usually after about two months of operation, a new one is quickly opened. So web page blocking is a rather labor intensive and inefficient way of restricting access to information within a country's borders. Blocking certain locations on the internet also does nothing to stop the email distribution of news from sources that change the address they send from daily, as VIP Reference News does.[50]

The kinds of threats described above may eventually be reduced as networks begin to grow and gain the resiliency that comes with having many nodes and lots of communication pathways, so sabotaging those pathways of electronic communication is impractical. It is important to note however that many groups in poor countries depend on a very few people to send and receive messages through the internet for them.[51] China's imprisonment of people facilitating the evasion of censorship suggests that people with internet access and contacts with oppressed groups may become the next target of governments seeking to disrupt such groups' communication with the outside world.

Another form of sabotage can be used when a group wants to provide a forum on the internet to let anyone speak, such as a petition or discussion hosted on a web page. The Chinese dissident Wang Dan hosts a petition on his web site calling for the Chinese government to change the official story on what happened during the protests at Tienanmen Square. Soon after he started the petition his site was flooded with "obscene messages and insults" for all to read. It is not known whether employees of the Chinese government were involved in this campaign of electronic heckling, but it is entirely possible. Such heckling attacks on an open forum could be used to drown out the exchange of information among those interested in human rights with the "noise" of obscenities and insults and the retaliatory remarks they are likely to provoke. It is possible to address this problem by taking editorial power over what people are permitted to say in such a forum, but doing so is extra work and may run counter to the principles of those deeply dedicated to freedom of speech.[52]

Governments troubled by the work of human rights groups frequently have the means and the motive to carry out the kinds of actions described under this pitfall. So surveillance and sabotage could become more frequent as governments become more aware of the power of coordinated action by activist groups. The U.S. Army, seeing the success of the Zapatistas in restricting the freedom of the Mexican army to use force, has conducted exercises that give cause for concern. In these exercises the Army attempts to stop an NGO that is trying, through coordinated protests and civil disobedience, to prevent or delay the U.S. entering into a war.[53] There should be public discussion over what ways of resisting pressure from activists are reasonable and which ways undermine the principle of democratic decision-making.

Conclusion

The following are the opportunities and pitfalls of new information and communication technology for Human rights NGOs:

OPPORTUNITIES	PITFALLS
Enhances the ability of human rights NGOs to marshal the facts to make a powerful case that rights violations are occurring and the perpetrators are known.	The proliferation of voices demanding attention for their human rights concerns might lead to a problem of too much noise interfering with effective action.
Enhances the ability of NGOs to draw other people into the group's organizing efforts and create connections through which to collaborate.	Some places are legally, socially, or economically unfavorable for the application of technology to human rights work.
Enhances the ability for NGOs to publicize events and attract global attention.	New technologies for communication and the processing of information create new vulnerabilities to surveillance and sabotage.

Given the complexity of the issues discussed in this paper it would unwise to try and predict whether these new technologies would, on balance, turn out to be a good thing or a bad thing for progressive social movements. If human rights groups continually fail to take steps to address the pitfalls above, the human rights groups' prospects look considerably less rosy than some of the more optimistic scholars believe. Movements could find their ability to communicate effectively with the public hindered because there are too many spokespeople and possibly also because of government disinformation campaigns. They could find themselves even more open to government spying into their activities. Many movements could find it legally or economically impractical to make full use of the technologies discussed here.

On the other hand, if human rights groups manage to take full advantage of the opportunities technology offers, the human rights movement will achieve more than they have in the past. Global attention will focus on humanitarian crises more quickly, longer and with more force than in the past, no matter how physically remote those crises are from the developed world. Human rights groups will be able to coordinate strategy globally and share moral and technical support as never before. Individual and institutional perpetrators of human rights violations everywhere will find it more difficult every year to successfully deny responsibility for their deeds.

The reality will probably be some combination of the above. It seems that many NGOs are aware of the opportunities and are beginning to exploit them. The question then becomes: how well will NGOs prepare to avoid the pitfalls and how hard will their enemies work to exploit those pitfalls. The work of this paper is far from complete. There needs to be an effort to apply knowledge of these opportunities and pitfalls to a range of cases of social movements, without the selection effect of just examining cases where use of technology has been fairly important or interesting. If enough such case studies are done, we would be on the way to developing a useful theory of information and communication technology's role in human rights work in a global context.

Notes

[1] Information Technology includes everything which serves the function of creating, acquiring, searching, editing, distributing, or sharing information in whatever form it may take, including audio, video, text, computer programs, or any combination thereof. The newer information technologies discussed in this paper fall roughly into three categories; computer technology, telecommunications technology, and media technology. Computer technology (aside from computers themselves and peripherals made for use with them) includes databases, spreadsheets, geographic databases (GIS), word-processing, as well as networking together of people so that they may share data easily. Telecommunication technology is involved with making communication (and, implicitly, computer networking) at long distances quick, convenient, and affordable. Telecommunication technology includes telephone systems, fax machines, two-way radio, the internet, communication satellites and satellite dishes. Relevant media technology includes VCRs, camcorders, affordable video editing/production equipment, low wattage radio stations, and desktop or web publishing. Such technologies allow for the quick, cheap, and effective representation of ideas or events.

[2] Carlos Alberto Afonso, "NGO Networking: The Telematic Way," *Development* 2 (1990).
Sheldon Annis, "Giving Voice to the Poor," *Foreign Policy* 84 (1991).
Sheldon Annis, "Evolving Connectedness Among Environmental Groups and Grassroots Organizations in Protected Areas of Central America", *World Development* 20, no. 4 (1992):591-592.
Howard Frederick, "Computer communications in cross-border coalition building: North American NGO networking against NAFTA," Gazette: The International Journal of Mass Communications Studies 50, no. 2/3 (1992).
Gladys D. Ganley, The Exploding Political Power of Personal Media, Norwood, NJ: Ablex, 1992.
Ganley, Gladys D. and Oswald H. Ganley, *Global Political Fallout. The VCR's first decade, 1976-1985*., Norwood, NJ: Ablex, 1987.
Robert Livernash et al., "Policies and Institutions: Nongovernmental Organizations: A Driving Force in the Developing World" in *World Resources 1992-93*, Washington, D.C.: World Resources Institute, 1993, p231.
Robert Livernash, et al. eds., "Policies and Institutions: Nongovernmental Organizations: A Driving Force in the Developing World," in *World Resources 1992-93*, Washington D.C.: World Resources Institute, 1993, pp.228-229.
"TV, VCRs Fan Fire of Revolution," Los Angeles Times, 18 January 1990.
Don Steinberg, "Panamanians use technology to balk censor", New York Times, 14 February 1988, p. 13.
Douglas Tweedale, "Noriega Faced With High Tech Opposition", UPI, 3 March 1988.

[3] Deeply influential in my conception of social movements as self-organizing informational entities was Karl W. Deutsch's *The Nerves of Government: Models of Political Communication and Social Control*, New York: Free Press, 1966. Also influential were parts of G.J. Mulgan's *Communication and Control: Networks and the New Economies of Communication*, New York: Guilford Press, 1991.

[4] Peter Willetts, ed., *Pressure Groups in the Global System*, New York: St. Martin, 1982: pp186-187, quoted in Alison Brysk, "From Above and Below: Social movements, the international system, and human rights in Argentina," Comparative Political Studies 26, no. 3, 1993: pp259-285.

[5] ibid.

[6] ibid., p261.

[7] This seems to agree with what Rucht has to say about environmental politics. Namely that expertise (linked to having high quality cognitive information) is displacing moral authority (linked to having high quality affective information) as the driving force behind policy. Dieter Rucht, "`Think globally,

act locally'? Needs, forms, and problems of cross-national cooperation among environmental groups", in *European Integration and Environmental Policy*, eds. J.D. Liefferink, P.D. Lowe and A.P.J. Mol, New York: Belhaven, 1993, p.90 quoted in Rodger A. Payne, "Sustainable Development and Transnational Resource Mobilization," unpublished manuscript, 1994:17. For an interesting alternative four-fold division of information-types into Media Symbolism, Science, (Global) Socio-Economic Context, and (details of the) struggle see Steve Breyman, "Knowledge as power: Ecology Movements and Global Environmental Problems" in *The State and social power in global environmental politics*, eds. Ronnie Lipschutz and Ken Conca (New York: Columbia University, 1993):140.

[8] Alison Brysk, "From Above and Below: Social movements, the international system, and human rights in Argentina," *Comparative Political Studies* 26, no. 3 (1993): 263-265, emphasis added. In the human rights case, sovereignty is thought not to be a defense since sovereignty is itself contingent on the state being the people's defender rather than oppressor. The monopoly of force within a state's borders is limited to legitimate force. (ibid., 265).

[9] *Environmental Politics in the International Arena*, ed. Sheldon Kamieniecki, (Albany, NY: SUNY, 1993): 266.

[10] ibid.

[11] For instance, "dataveillence" and camcorder surveillance are used both by NGOs against governments and by governments against NGOs.

[12] At the time of the interview Dan Salcedo was Human Rights Coordinator for the American Association for the Advancement of Science.

[13] El Rescate, "The Index to Accountability Project," mimeo, no date. Dan Salcedo, interview by author, Washington, D.C., 22 December 1994. This project was also described on page 841 of Patrick Ball, Mark Girourard, and Audrey Chapman, "Information Technology, Information Management, and Human Rights: A response to Metzl", *Human Rights Quarterly* 19, (1997).

[14] U.S. Department of State, Daily Press Briefing, DBP#70, May 28, 1999. Available on the internet at: http://secretary.state.gov/www/briefings/9905/990528db.html

[15] Sheldon Annis, "Evolving Connectedness Among Environmental Groups and Grassroots Organizations in Protected Areas of Central America", *World Development* 20, no. 4 (1992):591-592.

[16] Harry Cleaver, “The Zapatistas and the Electronic Fabric of Struggle”, available on the internet at http://www.eco.utexas.edu:80/Homepages/Faculty/Cleaver/zaps.html

[17] Howard Frederick, "Computer communications in cross-border coalition building: North American NGO networking against NAFTA," *Gazette: The International Journal of Mass Communications Studies 50*, no. 2/3, 1992, p.233.

[18] James N. Rosenau, *Turbulence in World Politics: A theory of change and continuity*, Princeton, NJ: Princeton University, 1990.

[19] Harry Cleaver, “The Zapatistas and the Electronic Fabric of Struggle”, available on the internet at http://www.eco.utexas.edu:80/Homepages/Faculty/Cleaver/zaps.html

[20] John Garrison, "Computers link NGOs worldwide," *Grassroots Development*, Fall 1989, quoted in Robert Livernash et al., "Policies and Institutions: Nongovernmental Organizations: A Driving Force in the Developing World" in *World Resources 1992-93*, Washington, D.C.: World Resources Institute, 1993, p.231. Carlos Alberto Afonso, "NGO Networking: The Telematic Way," *Development* 2, 1990, p.21. Harry Cleaver, “The Zapatistas and the Electronic Fabric of Struggle”, available on the internet at http://www.eco.utexas.edu:80/Homepages/Faculty/Cleaver/zaps.html

[21] Harry Cleaver, “The Zapatistas and the Electronic Fabric of Struggle”, available on the internet at http://www.eco.utexas.edu:80/Homepages/Faculty/Cleaver/zaps.html

[22] James N. Rosenau, *Turbulence in World Politics: A theory of change and continuity*, Princeton, NJ: Princeton University, 1990.

[23] Peter Willetts, ed., *Pressure Groups in the Global System*, New York: St. Martin, 1982, p.188.
[24] Steve Breyman, "Knowledge as power: Ecology Movements and Global Environmental Problems" in *The State and social power in global environmental politics*, eds. Ronnie Lipschutz and Ken Conca, New York: Columbia University, 1993.
[25] Ian Buruma, "China in Cyberspace", *The New York Review*, Nov. 4, 1999, p.9.
[26] Patrick Ball, comments at the panel titled "Analysis of Electronic Threats in a Human Rights Environment", AAAS Annual Meetings on February 19, 2000, Washington DC.
[27] Caryn Graves, interview with author, Nov, 2, 1999.
[28] Dan Salcedo, interview by author, Washington, D.C., Dec. 22, 1994.
[29] Patrick Ball, Mark Girourard, and Audrey Chapman, "Information Technology, Information Management, and Human Rights: A response to Metzl", *Human Rights Quarterly* 19, (1997).
[30] Clifford Bob, "Globalization and the Social Construction of Human Rights Campaigns", paper presented at the conference on Globalization and Human Rights, University of California, Irvine, January 15-16, 2000.
[31] Ronnie D. Lipschutz, "Reconstructing World Politics: The Emergence of Global Civil Society," *Millennium* 21, no. 3 (1992): 412
[32] ibid: 413
[33] For a different take on necessary conditions, see Rosenau's list of conditions for when states are likely to 'make room' for substantive NGO involvement. James N. Rosenau, *Turbulence in World Politics: A theory of change and continuity*, Princeton, NJ: Princeton University, 1990, p.306.
[34] Clifford Bob, "Globalization and the Social Construction of Human Rights Campaigns", paper presented at the conference on Globalization and Human Rights, University of California, Irvine, January 15-16, 2000.
[35] Elizabeth Fox ed., *Media and Politics in Latin America: The struggle for democracy*, Newbury Park, CA: Sage, 1988, p.139.
[36] David Ronfeldt, John Arquilla, Graham E. Fuller, and Melissa Fuller, *The Zapatista "Social Netwar" in Mexico*, RAND, MR-994-A, 1998, p.25. Available on the internet at http://www.rand.org
[37] Sheldon Annis, "Evolving Connectedness Among Environmental Groups and Grassroots Organizations in Protected Areas of Central America", *World Development* 20, no. 4 (1992):591
[38] Ian Buruma, "China in Cyberspace", *The New York Review*, Nov. 4, 1999, p10. *China News Digest-Global Newsletter*, January 21, 1999. Available on the internet at: http://www.cnd.org/CND-Global/CND-Global.99.1st/CND-Global.99-01-21.html
[39] This risk can be large or small depending on how well funded/sophisticated the relevant internal security agencies are and how much of a threat the government thinks a given movement is. David Banisar, "A Primer on Electronic Surveillance for Human Rights Organizations," *International Privacy Bulletin* 1, no. 3 (1993): 12-15. Wayne Madsen, "The Intelligence Agency Threat to Data Privacy and Security", unpublished manuscript for an article to appear in *The Journal of Intelligence and Counter-Intelligence*, 1993.
[40] Patrick Ball, introductory comments at the panel titled "Analysis of Electronic Threats in a Human Rights Environment", AAAS Annual Meetings on February 19, 2000, Washington DC.
[41] Encryption software uses complicated mathematics to scramble messages and files so only the intended recipient can decode and read them. But interception implies more than just learning what was said. There is also the opportunity to forge messages from movement members in a way that will disrupt the group's internal cohesion or operations. Alternatively, any or all e-mail or files can be prevented from being delivered or be altered in ways that may be difficult if not impossible to detect. But depending on the circumstances, the government can take an encryption code-key by force or guile to unlock all those scrambled conversations and correspondence they have saved, and of course

hidden microphones or human spies can nullify the benefits of encryption in certain cases. For a further discussion of the limitations of encryption, see the documentation file that is included with the PGP package. Note that even those at lowest levels of poor movements for whom encryption may not be practical can always resort to the 'poor-man's encryption' of talking in oblique language and metaphor. (Dan Salcedo, interview with author, Washington, D.C., December 22, 1994.)
As for the threat of voice conversations being wiretapped: Equally strong PGP-based encryption software for voice is available for those with computers with an added piece of hardware on both ends of the conversation. Some time later phones and faxes with encryption chips built in will become widely available.

[42] Patrick Ball, personal communication November 5, 1999. Also, comments made by Ken Ward, Oscar Hernandez, and Oliver Mazriegos at the panel titled "Analysis of Electronic Threats in a Human Rights Environment", AAAS Annual Meetings on February 19, 2000, Washington DC.

[43] HushMail is available on the internet at http://www.hushmail.com.

[44] Government agents in developing countries can at least get access to (if they don not already directly control) the computers of a human rights group's Internet Service Provider. So these agents could reprogram the ISP's computer to route connections intended for hushmail.com to a computer the under government control. This called a DNS (Domain Name Server) hijack. The user would see hushmail.com in their web browser's window showing what machine they were connected to, but they would not really be connected to that machine. To enhance the deception, government agents might be able to buy an electronic certificate from one of the many for-profit Certifying Authorities. CA's are organizations that a user's web browser trusts to tell the user who really owns the web page the user is connected to. If government agents get such a certificate and associate it with their fake HushMail page, the little lock icon on the user's browser indicating an encrypted connection will light up just like with the real page. This certificate, which the user might not bother checking every time, could include identifying information about the owner of the fake HushMail page that looks very similar to the identifying information for the owner of the real HushMail page. Carl Ellison, comments at "Analysis of Electronic Threats in a Human Rights Environment", AAAS Annual Meetings on February 19, 2000, Washington DC.

[45] Human Rights Watch, "Testimony on Human Rights and Encryption before the House Subcommittee on International Economic Policy and Trade: Tuesday May 18, 1999", available on internet at: http://www.hrw.org/hrw/advocacy/internet/testim-518.htm

[46] Graham Lane, personal communication, November 17, 1999.

[47] Oscar Hernandez, comments at the panel titled "Analysis of Electronic Threats in a Human Rights Environment", AAAS Annual Meetings on February 19, 2000, Washington DC.

[48] Shirley Christian, "Pinochet Foes Guard Against Fraud," *New York Times*, 13 September 1988, p. A3.

[49] Amnesty International, "Tunisia: Human rights defenders increasingly targeted", October 18, 1999, available on internet at http://www.amnesty.org/news/1999/53003599.htm

[50] Ian Buruma, "China in Cyberspace", *The New York Review*, Nov. 4, 1999, p.11.

[51] Harry Cleaver, "The Zapatistas and the Electronic Fabric of Struggle", available on the internet at http://www.eco.utexas.edu:80/Homepages/Faculty/Cleaver/zaps.html

[52] Ian Buruma, "China in Cyberspace", *The New York Review*, Nov. 4, 1999, p.10.

[53] Harry Cleaver, "The Zapatistas and the Electronic Fabric of Struggle", available on the internet at http://www.eco.utexas.edu:80/Homepages/Faculty/Cleaver/zaps.html