Brian Martin, *Social Defence, Social Change*
(London: Freedom Press, 1993)

12
Telecommunications for nonviolent struggle

by Schweik Action Wollongong*

Telecommunications can play a vital role in nonviolent resistance to aggression or repression. Yet there has been no systematic development of telecommunications research, policy or training for this purpose.

We interviewed a number of telecommunications experts to learn how the technologies could be used in nonviolent struggle. We report our general findings and list a series of recommendations for use and design of telecommunications. This pilot project reveals the radical implications of orienting telecommunications for nonviolent rather than violent struggle.

* This chapter is adapted from a paper by Schweik Action Wollongong. Those involved in the project were Sharon Callaghan, Terry Darling, Debra Keenahan, Alison Rawling, Lisa Schofield, Rosie Wells and myself. The group is named after the fictional character Schweik (or Svejk), a soldier who created havoc in the Austrian army during World War I by pretending to be extremely stupid. See Jaroslav Hasek, *The Good Soldier Svejk and His Fortunes in the World War*, translated by Cecil Parrott (Harmondsworth: Penguin, 1974).

Examples

Communications are absolutely crucial to nonviolent struggle against aggression and repression. The following cases illustrate some of the roles of telecommunications.

• Indonesian military forces invaded the former Portuguese colony of East Timor in 1975. Their occupation led to the deaths of perhaps a third of the population through killings and starvation. By cutting off communications to the outside world, outrage over this repression was minimised. The Australian government aided in this communications blockade by shutting down a short-wave transmitter in the Northern Territory.

In November 1991, a massacre of nonviolent protesters in Dili, the capital of East Timor, rekindled international concern over Indonesian occupation of East Timor. This killing attracted attention because of the presence of foreign observers and videotapes of the killings, illustrating the importance of communications in generating opposition to repression.

• In Spain there was an attempted military takeover in February 1981; rebels occupied parliament and held 300 parliamentarians hostage for 17 hours. King Juan Carlos appeared on television and denounced those responsible. This act was vital in undermining support for the uprising.

• In December 1981 there was a military coup in Poland, aimed at stifling the Solidarity workers movement. The coup was accompanied by severing of radio and telephone links with other countries for several days, until the takeover could be sustained.

• In 1989, Chinese troops massacred hundreds of pro-democracy protesters in Beijing. In the aftermath, the Chinese government tried to cut off telecommunications to other countries. But fax machines continued to operate, providing information to outsiders and enabling informed overseas protests. When the Chinese government publicised a telephone number for reporting of "dissident elements," this information was leaked overseas, and people from around the world jammed the number by making continual calls, preventing it from being used for its original purpose.

• The Soviet coup in 1991 failed, in part, due to lack of control over telecommunications. Yeltsin's supporters got out the basic message—refuse to cooperate with the coup leaders and defend the

Russian parliament—using radio, faxes, computer networks and leaflets.

• The peace movement in former Yugoslavia makes excellent use of fax and computer networks. For example, a message may be faxed from an antiwar group in Sarajevo to Zagreb, where it is quickly translated into English and put on a computer bulletin board, thus getting information from Sarajevo to thousands of people in a matter of hours.[1]

Telecommunications also played a big role in resistance to the 1961 Algerian Generals' Revolt, the 1968 invasion of Czechoslovakia and the 1987 Fiji coups, as described in earlier chapters. These examples show the crucial importance of communications in nonviolent resistance to aggression and repression.

Killings of unarmed civilians can generate enormous outrage, both in local populations and around the world. By contrast, the killing of guerrilla fighters gains relatively little attention—violence against violence is seen as legitimate, even when the sides are unevenly matched. But killing or beating of civilians has to be publicised. If repression is carried out in secret, there is little impact. Communications and publicity are vital.

The project

Schweik Action Wollongong is a small voluntary group of people who work on projects relating to social defence. Various members of the group are also active in other social movements as well as holding down regular jobs. We keep in regular contact with like-minded individuals and groups throughout Australia and overseas.

Our project on telecommunications and social defence commenced in mid 1990. We interviewed a diverse range of people from the areas of satellite communications, computer engineering, ham radio, computer systems development and community radio. We started by interviewing people we knew and branched out as we asked the people interviewed who else we should be contacting. The interviews were usually conducted by two members of our group, one of whom took notes. The notes were written up and circulated

---

[1] Information from Christine Schweitzer.

amongst members of the group. Care was taken to ensure the anonymity of the interviewees.

From our point of view, the interviews had a very useful two-fold purpose. Not only were they a valuable and interesting source of information on telecommunications capabilities, but they also allowed us to talk to other people about social defence. In this way the interviews were a goal in themselves, namely raising the issue of social defence, as well as a method for gaining information about telecommunications for nonviolent struggle.

Main results

We describe some of our main findings according to the type of technology used.

The **telephone** system is a wonderful means for mobilising against repression. It is readily available to nearly everyone, requires very little knowledge or training to use, and can be used to contact virtually any part of the world. Most importantly, it is a network means for communication. Anyone can contact anyone and there is no central control or censorship over what people say on the phone.

There are two important limitations to the telephone. First, it can readily be tapped, and individuals usually don't know when this is happening. Tapping can do little to stop large-scale opposition, because there must ultimately be people who listen to tapped conversations. If there are enough people in the resistance, the regime can monitor only a small fraction of relevant calls. Tapping in this situation is effective mainly through its psychological intimidation of callers who think someone is listening to their conversations.

A simple way to get around tapping is to use public telephones or simply a friend's telephone. For answering of phones, some of the systems which forward a call to another number are useful: the location of the person answering the phone is not readily known to the caller (or someone listening in). Also worth considering, as preparation for emergency situations, are machines that change the pitch and vocal quality of a voice, and encryption technology (which puts the message into code).

The second limitation of the telephone system is that it can be cut off selectively or entirely. This can be used against the regime

or the resistance, depending on loyalties of technicians on the inside. Generally, the resistance would be wise to keep the telephone system operating. For that matter, any modern industrial society depends on telephones for everyday functioning. So it is unlikely that the entire system would be cut off except for short times, such as the aftermath of a coup or massacre. Resisters should build links with technical workers to ensure that the chance of this is minimised.

Fax is an extension of the telephone system to printed documents. All the same considerations apply, except that documents received are often available to anyone who happens to be around. Faxes with security codes overcome this problem. (This is similar to the lack of security in telephone answering machines.) Fax machines are much less common than telephones and require a bit of training, but are basically easy to use. Using faxes is much better when lengthy or complex information needs to be sent out.

Computer networks are excellent for person-to-person communication, but can also be used to send messages to several addresses at once, or put material on a computer bulletin board for all to read. They have the same limitations as the telephone system, namely the potential for being monitored or cut off by a master user (the person who controls the system and knows all the passwords).

Unlike telephones, computers are not so easy to use and are available to only a small fraction of the population, being relatively expensive. Computers are becoming cheaper, more widely available and more user-friendly each year, and will undoubtedly play an increasing role in communication in crisis situations.

In the case of emergency, it would be advantageous to be able to run computer networks on a different basis. For example, the master user's power to shut down or monitor accounts could be terminated. Such a change could be programmed to occur, for example, whenever a specified number of users inserted a special command within a certain time interval. The methods of doing this, and their implications, remain to be studied.

Computers have the capacity to store vast quantities of information, and this leads to new considerations. Some databases—for example, containing information on social critics—would be sought by a regime. One possibility would be to have plans to hide, encrypt or destroy sensitive information in case of emergency.

Short-wave radio is another excellent network form of telecommunications. It can be used to talk person-to-person from different parts of the globe. Furthermore, it operates as a stand-alone system, so that the plug cannot be pulled from any central location.

Calls on short-wave can be overheard by others with suitable equipment; as in the case of telephone, the more people who are using the medium, the less the risk to any one. The location of short-wave transmitters can be pinpointed, but the transmission site can readily be moved. An ideal way to ensure continued international communications in a crisis would be to have a short-wave system in every home, plus many additional public systems for anyone's use.

A combination of short-wave transmission and computer data produces packet radio, in which packets of data are transmitted. These transmissions cannot be listened in on, though they could be deciphered with special equipment. Packet transmissions can be sent up to amateur radio satellites and broadcast down to receivers later, even halfway around the world. Combined with encryption, this provides a highly secure method for sending masses of data.

The main limitation of short-wave radio is the limited availability of the technology and knowledge of how to use it.

CB radio is similar to short-wave radio, except for a much more restricted range.

Television and **mainstream radio** are much less useful against a repressive regime. Indeed, they are prime targets for takeover. The main reason is that a few people control the content and the transmissions; everyone else consumes the message. In this situation, the loyalty of both technicians and broadcasters is crucial. If stations are taken over, perhaps the best counter move would be for technicians to cause faults hindering transmission. But this cannot be the basis for a programme of resistance, since immense pressures can be applied to recalcitrant staff, or new compliant staff brought in.

With some advance planning, a takeover could be delayed and hindered for at least days or weeks, if not resisted indefinitely. But often the threat is not immediately recognised by all workers, so it can be difficult to obtain agreement for such action.

Community radio stations, in which community groups control programme content and participate in making station policy, are much better placed to continue speaking out. Preparations for

emergencies at such stations have the added advantage of making many groups aware of the necessity for action in a crisis.

In the longer term, it would be desirable to reduce dependence on the broadcast technologies of television and mainstream radio and to increase the use of network technologies such as telephone.

It is important to remember that other forms of communications are important besides telecommunications. This includes talking face-to-face, leaflets, bulletin boards, graffiti, posters and the ordinary post. Telecommunications can aid resistance to aggression and repression, but they are not essential.

It is also important to remember that technology is useless unless people are willing to act. In this sense, politics, not technology, is the key to resistance.

Recommendations

Even with the present state of technology and people's awareness, telecommunications can be an important part of nonviolent resistance to aggression and repression. But there are also ways to improve the effectiveness of telecommunications for this purpose. We list them here under five categories.

Realising present capabilities. Right now, people are quite capable of using existing telecommunications to oppose a repressive regime. People need to be made aware of their own capabilities.

If the mass media of television and mainstream radio, plus large-circulation newspapers, are taken over, there are still plenty of avenues for independent communication. The telephone system is the most obvious. People need to realise that only a small fraction of phones can be effectively monitored. Those who are at greatest risk of being monitored should realise the possibilities for using other phones.

Those who have access to computer networks should be made aware of the potential for communication. This includes people working for banks, universities and large companies. Similarly, short-wave operators should be made aware of the crucial importance of their technology.

Technicians in vital areas—such as television broadcasting or computer networks—need to be aware of how they can help maintain communications among those resisting repression.

Learning to use existing technology. Most people know how to use telephones. Many more can learn how to use fax machines and computer networks. Run a practice session with friends.

An even greater commitment is needed to learn to use short-wave radio or packet radio. It is important for these skills to be more widely shared in the community.

Preparation. Knowing how to use telecommunications is one thing; being prepared to use them in a crisis is another.

Having a procedure for telephoning people in an organisation or network is important. The system should work even when some people are not available or some telephone lines are interrupted.

Developing lists of fax numbers is another useful step. On a computer network, lists of important contacts could be kept ready for an emergency, and perhaps hidden in a coded group so that others cannot inspect the list.

Another important part of preparation is simulations. A group of people can run a drill, testing out their communication systems in the face of a few disrupters. In this way the strengths and weaknesses of different systems can be tested. Also, people can become accustomed to acting promptly and sensibly in a crisis situation.

Designing technology. Telecommunications systems should be designed to provide maximum use to a popular, nonviolent resistance, and minimum help to a repressive regime. This seems never to have been a consideration in system design before, so it is difficult to be precise about what is required.

Is it possible to design a telephone system so that a speaker is warned if another party is listening in on a call? Is it possible to design a telephone system in which every phone can become—at least in emergencies—as nontraceable as a public phone? Is it possible to design a telephone system so that user-specified encryption is standard? Or in which encryption is introduced across the system whenever a specified fraction of technicians (or users) signal that this is warranted?

Is it possible to design a computer network so that the master user's control over accounts is overridden when a certain fraction of users demand this within a specified period? Is it possible to design a computer system in which encryption or hiding of data bases is automatic when there is unauthorised entry?

There are many other such questions. Perhaps, too, these are not the appropriate questions. The most effective design of a telecommunications system to operate against a repressive regime will depend on practical tests which cannot all be specified in advance. It is certainly the case that there are a host of difficult and fascinating design problems.

It is important to remember that the design is not simply a technical issue, since the most effective design depends on an assessment of people's skills, commitment and behaviour in a crisis situation. Good design will discourage aggressors and encourage resisters. In this context, being seen to be effective is part of what makes a system effective in practice.

Organising society. Telecommunications is only one part of nonviolent resistance to aggression. Other areas are important too, such as energy, agriculture and industry, as described in other chapters.

Whether the changes in the organisation of society involve production of goods or political decision-making, there are implications for communication. For example, if a regime tried to repress dissent by interrupting deliveries of food, then it would be vital to have reliable communication about available supplies, local gardens, needy people, etc.

All this would require preparation, organisation, commitment and training.

We found the telecommunications project stimulating and challenging. We learned a lot about telecommunications and also about interviewing. By working in a group, we learned from each other and provided support for keeping the work going.

The telecommunications project is just one of an enormous number of possible community research projects. Some other groups that could be approached are salespeople, clerical workers, factory workers, transport workers, school students, teachers, workers in the building trades (including plumbers, carpenters and electricians), actors, health workers, farmers, police and soldiers.