D I S C U S S I O N   P A P E R   O N   E C C   S E C U R I T Y

1. Introduction

Under the current State of Emergency, security has become an integral part of our organisation. ECC members have experienced much harassment over the past months. Over forty five of our members have been detained and several have been served restriction orders. Many of our National Committee members have been in hiding to avoid detention. Countless ECC houses have been raided by Security Police and one house in Jo'burg was petrol-bombed.

ECC itself was singled out for particular restriction in the Emergency Regulations, and in various regions was subjected to further restrictions that amounted to banning.

In this context we tightened up on our security considerably. This discussion paper attempts to draw together some of the lessons that we've learnt. It is based largely on a security memorandum that the Cape Town Exec. drew up in September '86

The paper is not intended to be prescriptive but simply to serve as a basis for security discussions. What is most important is that such discussions are seen as on-going by regions. What we have experienced could easily happen again, and quite possibly happen in an even more serious way.

Although ECC is a legal campaign, operating within the law to change military-related legislation, it is seen by the State as a threat to be rendered ineffective. It is not unlikely that ECC will experience further harassment.

We need to be prepared.

2. Anticipation

Despite the harassment and initial shock of the Emergency, ECC was able to weather the storm extremely well. This was largely because we had, at a national and regional level, anticipated a big clampdown happening at some stage.

We need to be similarly prepared for another clampdown. For example, we need to work out in advance how to get together very quickly but safely if the need arises, and how to maintain communication links under repressive conditions.

3. Maintain a high level of security

The key element to the State's harassment of ECC is close surveillance of our activities. It is vital that we make the surveillance as difficult as possible.

a) Telephones

Wherever possible avoid using the phone. When arranging meetings, action and preparation for action, the phone sould <u>never</u> be used. This principle should be followed religiously <u>whatever</u> the content of the meeting and <u>whoever</u> is going to attend. If a meeting is raided or an action bust, it is crucial that we are able to identify the probable cause (see later). Never use the phone to or from a safe venue and never mention on a phone the name of someone in hiding.

We know that Branch regularly tap phones and gain a wealth of useful information. We also know that phones are used to listen to conversations in the vicinity in which the phone is located. When the phone is 'down', the speaker part of the phone is not disconnected like the 'listening' part is (note the profound, technically advanced terminology). Detainees have often been confronted with tapes of personal conversations with lovers, et cetera. It is not difficult to see how this could be used to pressurise them.

We know that computer systems attached to telephone exchanges allow for the similtaneous monitoring of thousands of calls. So don't assume that no-one would ever bother to tap your phone!

b) Secure venues

When setting up meetings we should, as far as possible, do so in a secure way:
* have an initial meeting place and have a safe venue;
* everyone must arrive <u>dead</u> <u>on</u> <u>time</u> at the meeting place;
* people must watch for being followed to a safe venue and should park their cars some distance from it;
* people should leave the safe venue together and not in dribs and drabs;
* safe venues should never be discussed indoors.

All this obviously makes for a lot of extra effort and also contributes to difficulties of integrating and involving 'new' people (see later). However, at some point in the future we may <u>have</u> to organise <u>all</u> meetings in this way, so where it is viable we should get used to it.

This is not to say that all sub-com meetings should be organised like this - people should assess if it is appropriate.

c) Social arrangements

Chaos in our organisational arrangements is almost always the main cause of security breaches. <u>Everyone</u> should know <u>where</u> they are meant to be at <u>what</u> <u>time</u>. Material needed for meetings or workshops should be at the venue so that we can avoid rushing back and forth. Messages shouldn't be left for people to connect with meetings. Generally, the point is that everything must be organised properly and beforehand.

d) Written notes

No one should take notes at a meeting without the agreement of the group as a whole. It's a good idea to decide at the start of the meeting whether people can take notes and to

what extent.

If notes are going to be taken, they should avoid mentioning people's names.

People should also be careful with diaries that have meetings and venues written in. It's a good idea to tear out pages as the days pass.

Written material and notes should, as far as possible, be destroyed after they are no longer needed. Often notes seem innocuous but in fact can provide important information and an entry point for interrogation.

Again we should stress that the notes <u>are</u> innocuous and our work <u>is</u> completely above board, but this makes little difference to an insecure State.

4. Keep your house in order

Because the security police cannot find anything illegal in our ECC activities, they will look for other ways to bust us. A favourite way is to raid houses and search for banned literature and drugs. So make sure your house is clean.

5. Maintain cohesion; resist paranoia

State harassment has several purposes. One is that we become frightened and are either put off politics ar at least seriously limit our activities.

When the heat is on, maintaining organisational cohesion and solidarity is one of our most urgent tasks. We need to deal with feelings of fear, despair and isolation. We must create the space for people to talk about how they are feeling and to give each other support.

We also need to watch for paranoia - for over-reacting or panicking. The trick is to find just the right level of security to protect ourselves and at the same time to keep working.

6. Spies

Informers in organisations like the ECC are an obvious potential problem. As damaging as a spy can be, the way in which suspected spies are dealt with is sometimes even more damaging to the organisation.

Above all, we must avoid spy-mongering - undisciplined skinner about so-and-so. This kind of discussion alienates people and sows mistrust. It is exactly the kind of thing the Security Police like to encourage.

Everyone in the organisation must know that if they suspect someone of being a spy, they should raise it with an exec member they trust <u>and with no one else</u>. Within the exec it can be discussed further.

7. Democracy, integration and security

One of the biggest problems with a high level of security is that is is difficult for new members to join and get involved in our organisation. People might be suspicious of new members, new members might be alienated by the high level of security, et cetera. Sub-coms need to discuss ways of coping with this problem. Close personal contact with individuals is one way of getting around the problem, but there are probably other ways of organising things so that people can feel at home quicker.

A related problem is that the democratic processes within ECC are effected by tighter security. In Cape Town and Jo'burg when we first assessed how we were handling the Emergency, one of the things that was raised was the centralisation of discussion in the executive. We may need to use the exec from time to time to have particularly sensitive discussions, but there need never be a situation where discussion about ECC and its future is centralised. As much as we need to watch the exec to see that it doesn't overstep its mandate, we have to be equally vigilant that sub-coms are feeling responsible for and thinking about the whole of ECC and not just their own particular area.

8. Know you rights

Because there are literally hundreds of laws that can be used against democrats, we have to know what we can and cannot do. We should be familiar with the Emergency Regulations, the Internal Security Act, the relevant sections of the Defence Act and the regulations concerning picketing, pamphleteering and postering.

Knowing what we can and cannot do gives people confidence and prevents unnecessary mistakes being made.

If there is doubt about the legality of some aspect of our work, consult a lawyer. We must be careful though not to let our lawyers make our decisions for us. The lawyer will give legal advice - we still need to make political decisions. Often the lawyer will not be able to give you a definite answer because of the vagueness of so many laws. If in such a situation a region wants to take a risk that has national implications for ECC, it must consult other regions first.

9. The Future

Much of this may seem out of place with the current level of harassment of ECC. We have been able to hold public meetings and engage in other public activities, the state does not seem to be looking for any of our members, almost all our detainees have been released and our general decision making forums are working.

However, everything we have seen and said until now points to a gradually worsening climate of repression. Survival under these conditions depends entirely on whether we have been trained adequately and on whether our organisation is structured in the best way. We mustn't be lulled into a false sense of security by the apparent loosening up. It is possible that harassment will increase when ECC embarks on another national campaign.

We should as far as possible be using this time to prepare for
more repressive conditions.

LN Nov '86