Statewatch analysis

EU agrees rules for remote computer access by police forces – but fails, as usual, to mention – the security and intelligence agencies

by Tony Bunyan

The issue of state agencies getting “remote access” to computer hard drives came to light in June 2008 when the German government adopted a new law to give its main police agency this power in terrorist investigations.[1] This amended the Federal Criminal Police Office Act to allow judicial authorisation to conduct online remote computer hard drive searches (and video surveillance in private homes) in "cases of terrorist threats" to allow:

> *the surveillance of private homes and telecommunications as well as remote searches of computer hard drives*

The technology that might to be used when accessing a hard drive could be Trojan software or “Rootkits” (which remain quietly hidden from the computer owner while accessing and spying on the content) but more likely what is called “Remote Forensic Software" developed by a number of state agencies[2].

The position in Germany is public but what is happening elsewhere? The lack of legal powers has never stopped security and intelligence agencies in the UK (or the USA) from exploiting new technologies - if it is technologically possible then use it is the agencies’ rationale.[3] For from the 1970s British Telecom gave details of phone-calls to MI5 (internal security agency), MI6 (external intelligence service) and Special Branch on request – a power only made lawful under the Regulation of Investigatory Powers Act (RIPA 2000). Under RIPA police and security agencies can get access to communication data (“traffic data”) for example, a listing of e-mails sent and received and who they are from – but not the content which requires separate authorisation through a specific case warrant. However, they have the technical ability to enter any service provider, search for a “target” and get access to traffic data and the *content* – which of course they do, even though it is not lawful. Moreover, in the UK the agency which would handle remote computer access is GCHQ (Government Communications Headquarters), which works closely with the USA’s NSA and is part of the Echelon network.

So the question is who else is using “Remote Forensic Software” to remotely access computer hard drives through which state agencies can both “spy” on the user and also add or change content?

The EU initiative on remote access

On the 11 July 2008 the EU Council Presidency circulated a Note on a: *"Comprehensive plan to combat cyber crime"* to COREPER - the Council committee of Brussels-based high-level representatives of each Member State (EU doc no: 11784/08).[4]

Under the sub-heading "The emergence of new issues" it said that there were some: "projects already in existence" which require "common approaches" including:

> *the area of remote computer searches, **which are a delicate issue because of their cross-border nature**. (emphasis added)*

Reading between the lines the phrase: "projects already in existence" implies that state agencies in some Member States are already conducting cross-border remote computer searches both in their home countries and across borders in other states.

This Council Presidency Note of 11 July was very swiftly transformed into a proposal for formal Council "Conclusions". The penultimate version (EU doc no: 13567/08) refers to:

> *measures to facilitate remote computer searches, allowing investigators rapid access to data [5]*

The adopted version, which slipped unnoticed, and un-reported, through the November Justice and Home Affairs Council as an "A" Point (adopted on the "nod" without discussion, EU doc no: 15569/08) is more diplomatic saying:

> *facilitating remote searches if provided for under national law, enabling investigation teams to have rapid access to information, with the agreement of the host country [6]*

There is no mention of the "*delicate issue"* of *"cross-border"* searches, nor would anyone reading this adopted version (and not having seen the two earlier documents) necessarily realise that "remote searches" refers to "remote computer searches".

The caveat that these searches have to be "provided for under national law" and be carried out "with the agreement of the host country" suggests lawfulness and accountability. However, these "Conclusions" explicitly concern Treaty-based EU "police and judicial cooperation" *not* the security and intelligence agencies who are nowhere mentioned (see below). The "Conclusions" are not limited to terrorism but extend to the whole field of police and judicial cooperation.

The concept of "cyber-crime" currently covers scams such as "phishing" (getting confidential information from victims); terrorism; child pornography and attacks on

information systems. However, the stated intention is to extend these categories to "other areas" - one such extension is to cover "material [that] glorifies violence and terrorism".

Council "Conclusions" are policy statements which lay down markers for any future policies put forward by the European Commission. They are non-binding ("soft law") but they do enable (legitimate) any or all EU Members States and their agencies to introduce measures to "facilitate" remote computer searches at will.

G6 plus USA

Remote access to computer hard drives came up again at the G6 meeting in Bonn on 26-27 September 2008. G6 is an intergovernmental group comprised of the Interior Ministers of the six largest states in the EU – the only documents ever released are Press releases or set of Conclusions.[7] At the Bonn meeting they were joined by the Secretary of Homeland Security from the USA.

Arguing that the terrorists' use of modern technology required effective counter-measures:

> *The interior ministers note that almost all partner countries have or intend to have in the near future national laws allowing access to computer hard drives and other data storage devices located on their territory. However, the legal framework with respect to transnational searches of such devices is not well-developed. The interior ministers will therefore continue to seek ways to reduce difficulties and to speed up the process in future (para 13).*

Let's break this statement down. First, "almost all partner countries have or intend to have" laws allowing remote access to computer hard drives - the only country to have a law, passed after this meeting, is Germany. "Almost all" suggests most of the six intend to bring in such laws. If "almost all" intend to introduce laws allowing remote access this means they all have the technological capacity to carry out such searches now. How many are already carrying these out?

Second, we are told that the "legal framework" for "transnational searches" is "not well-developed", shorthand for non-existent. "Transnational searches" of computer hard drives do not require the physical presence of an officer/agent to enter a property as they are carried out "remotely" through the ether. The norms of traditional police cooperation, where one EU state requests information or data from another state, are to be put in place – but the security and intelligences agencies have few, if any, legal restraints placed on them compared to law enforcement agencies (LEAs).

Third, as the US Secretary for Homeland Security was sitting at the table it might reasonably be assumed that US agencies have exactly the same technological capability, indeed it would be extremely naive to assume otherwise. This leads to an obvious conclusion, if an Italian security agency can remotely access a computer hard drive in Spain, then US agencies can remotely access any computer in the EU.

How security and intelligence agencies avoid the limelight

In the UK remote computer hard disk searches are not covered by the Regulation of Investigatory Powers Act 2000 – it does allow the physical entering of premises/vehicles/offices to place "bugs" (listening devices) but not remote computer access by security and intelligence agencies.

This glaring "gap" is reflected in the EU where there is hardly any mention of internal security agencies in the 27 member stares.[8] The Framework Decision on data protection for the exchange between member states of information/intelligence expressly *excludes* internal security (and intelligence) agencies. Nor is there any reference to them in the Schengen Information System (SIS) or SIS II rules or indeed any of the EU/EC Treaties. "Out of sight" goes hand-in-hand with lack of accountability.

A few changes are happening in the post 11 September 2001 world where a limited degree of visibility legitimates their surveillance of "suspect communities" across the EU which, in turn, has led to LEAs working more closely with internal security agencies.

If the Lisbon Treaty is adopted a new EU Standing Committee on internal security (COSI) will be set up to deal purely with "operational matters" – a sure sign that its deliberations will be kept secret. More ominously Article 61 F of the Lisbon Treaty says:

> *It shall be open to Member States to organize between themselves and under their responsibility forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security.*

In the longer term the Lisbon Treaty (if adopted) would see the creation of a European External Action Service with EU embassies gathering intelligence – leading to an enhanced role for the Council's Joint Situation Centre (SITCEN).[9]

Conclusion – on the road to "total tyranny"

There are two broad categories of surveillance: *mass surveillance*, for example, the gathering of travel details on all air passengers in the EU or mandatory data retention of everyone's communications and *targeted surveillance*. Initially at least the use of remote access to computer hard drives will be used by the security and intelligence agencies against specific targets. However, as the scope of targets is extended to those who present a perceived danger to the state this could include lawyers working on contentious cases spied on or journalists working on sensitive stories or protest groups planning a demonstration.

A quote from Senator Frank Church who headed a seminal inquiry in 1975 into the surveillance of the peace movement in the USA (the "Church Committee report") seems pertinent:

> *If a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of government to know. Such is the capacity of technology.*

And that was more than 30 years ago.

This analysis first appeared in Statewatch Journal, vol 19 no 1. This version with links, August 2009

Footnotes

1. German Interior Ministry:
http://www.statewatch.org/news/2008/jun/germany-surveillance-powers-proposals.pdf

2. See on Rootkits: http://www.5starsupport.com/tutorial/rootkits.htm

3. The "security and intelligence agencies" (SECINT) are quite distinct from the "law enforcement agencies" (LEAs which include police, immigration and customs) in powers, remit and "need to know".

4. http://www.statewatch.org/news/2009/jan/eu-remote-computer-access-11784-08.pdf

5. http://www.statewatch.org/news/2009/jan/eu-remote-computer-access-13567-08.pdf

6. http://www.statewatch.org/news/2009/jan/eu-remote-computer-access-15569-08.pdf

7. The first meeting of the G5 – Germany, France, Italy, Spain and UK (before Poland joined the Group in 2006) was held in France in October 2003: see:
http://www.statewatch.org/news/2008/nov/g6-usa-sep-08.pdf

8. A rare exception is the EU measure on who can access the Visa Information System and for what purpose.

9. SITCEN was set up in 2005 on the authority of Mr Solana, Secretary General and High Representative of the European Council.