Europe spikes spooks' e-mail eavesdrop bid

US and British intelligence agencies received a major blow last week, when the EC urged governments to introduce uniform and effective encryption standards to protect communications on the Internet

By Duncan Campbell
Guardian, 15 October 1997

In a landmark report, the EC asserted that legal recognition and standards for digital signatures, which depend on effective cryptography, should be put in place across the EU by 2000 "at the latest".

The EC report, Ensuring Security and Trust in Electronic Communication [http://www.ispo.cec.bei/eif/policy/97503.html], is set to receive enthusiastic IT industry backing, after years of foot-dragging by the US National Security Agency (NSA) and the last British government in an attempt to block effective international encryption and keep Net communications accessible to their global surveillance systems.

Since 1991, the Clinton administration has been trying to persuade its citizens and allies to adopt a system for secret government access to private code keys. A heated battle is now underway in the US Congress, where five competing and opposing versions of an encryption law have been passed in different committees.

But Europe is having no truck with this. The EC report maintains that allowing third parties secretly to decode personal and business communications will not merely fail to stop criminals, but will create massive new security headaches. It would also threaten personal data privacy, already protected by a European directive on data protection. What's more, says the report, it would intolerably damage European interests in electronic commerce and the information society.

Although the EU concedes that individual governments can, in principle, make their own national security arrangements, member states are now being warned that restrictions on importing or exporting cryptographic products may be unlawful under sections of the European treaty, as well as contrary to existing community directives.

"The European Union simply cannot afford a divided regulatory landscape in a field so vital for the economy and society," the Commission maintains. "Divergent and restrictive practices with regard to cryptography can be detrimental to the free circulation of goods and services within the internal market" and will "hinder the development of electronic commerce".

To back this up, the EC has set a fast-paced timetable, which kicks off before the end of the year with an Internet Forum and the liberalisation of national and international restrictions on selling cryptography products. The EC has already decided in principle that member states should be required to guarantee "the free movement of encryption technologies and products" within the EU.

The Commission plans to hold an international hearing at the beginning of next year on this month's proposals, to be followed up by a directive on digital signatures. By 2000, the goal is to have a "common framework on cryptography in place throughout the Union".

The Commission says it found no evidence that regulation could or would stop criminals from using effective encryption. On the contrary: "Restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks."

Even more dangerous, says the EC, is the current US plan to build central depositories for private code keys. Such a system was also proposed in the UK a few weeks before the general election. The EC says this would give criminals "additional ways to break into a cryptographic system" and that the central key stores themselves would or could "become target for attacks" by organised crime or hostile intelligence agencies.

Europe's determination to press ahead with genuinely secure privacy and digital signature systems now threatens to put the US into third place, after Europe and Asia, in the race to exploit electronic commerce.

Opponents and advocates of effective cryptography agree that key access systems will fail entirely if introduced only in one country, as users will obtain secure cryptographic services from countries that do not have such restrictions. Electronic isolationism is not an option for an industrialised nation in the 21st century.

If US intelligence agencies continue to demand universal access to keys, they will not merely imperil their own citizens' privacy and constitutional rights, but gravely undermine the US lead in IT. Faced with increasing industry, international and civil liberties opposition from right and left, intelligence agency advocates have reached levels of hysteria not seen since the peak of the cold war. Three months ago, FBI director Louis Freeh told the US Senate Judiciary Committee that "uncrackable encryption will allow drug lords, spies, terrorists and even violent gangs to communicate about their crimes and their conspiracies with impunity". The public safety of our citizens was at stake, he insisted.

One official response to the EC report in Washington last week was a claim that corporations wanted key access systems in order to check on their employees' private e-mail messages. But this latest shift of tack only emphasises how out of touch US policymakers are. It is already clear in Europe that, whether or not companies might want to, it is unlawful for them to spy on their employees' private communications. That issue was settled six months ago in the European Court of Human Rights, when former Merseyside assistant chief constable Alison Halford was awarded damages against her former employers, who tacitly conceded that they had tapped her office telephone.

In Britain, advocates for restricting cryptography have spoken, almost wishfully, of the possibility of "a backlash" which would turn public opinion their way, "if there are serious crimes committed and people killed and encryption is in use".

Such scenarios are lampooned by experts of the seniority of Cambridge's Professor Roger Needham, now also Microsoft's Director of Research, who last month described the US plans as: "Like requiring men waving red flags to walk in front of horseless carriages. Strong and effective encryption systems can't be stopped."

British policy on encryption is now "up for grabs", say insiders. "There are only a limited number of moves that a government can make in a democratic society," DTI information security specialist Nigel Hickson told last month's Cambridge conference on economic crime. "We are still thinking what they can be."

Meanwhile, Labour IT minister Barbara Roche has taken delivery of an assessment of responses to the former government's proposals. DTI officials are taking comfort from the support they received for digital signature schemes, in contrast to the opposition and abuse engendered by the proposal for government access to keys. Both of these features have been intensified by last week's EC report.

The DTI now appears to be in favour of separate plans for digital signatures from the "law enforcement" agenda to restrict cryptography, and to press ahead with the former. It is confident of political and industrial support for this approach. Until last week, that left the question of a cryptography policy open, making British as well as US policymakers' offices potentially the site of trench warfare between clandestine agencies and the powerful IT lobby.

At an extremely timely moment, Europe has lifted the Government off the horns of that dilemna. Its clear and fast timetable, coupled with a firm warning that no European state may go it alone, the EC has not only pushed the spooks away but given the Government the chance next year to win substantial EC financial backing for Britain's IT industry in pioneering the new cryptosystems Europe should have in place for the millennium.

[Duncan Campbell is a freelance writer and broadcaster, and not the Guardian's crime correspondent of the same name]

15 October 1997