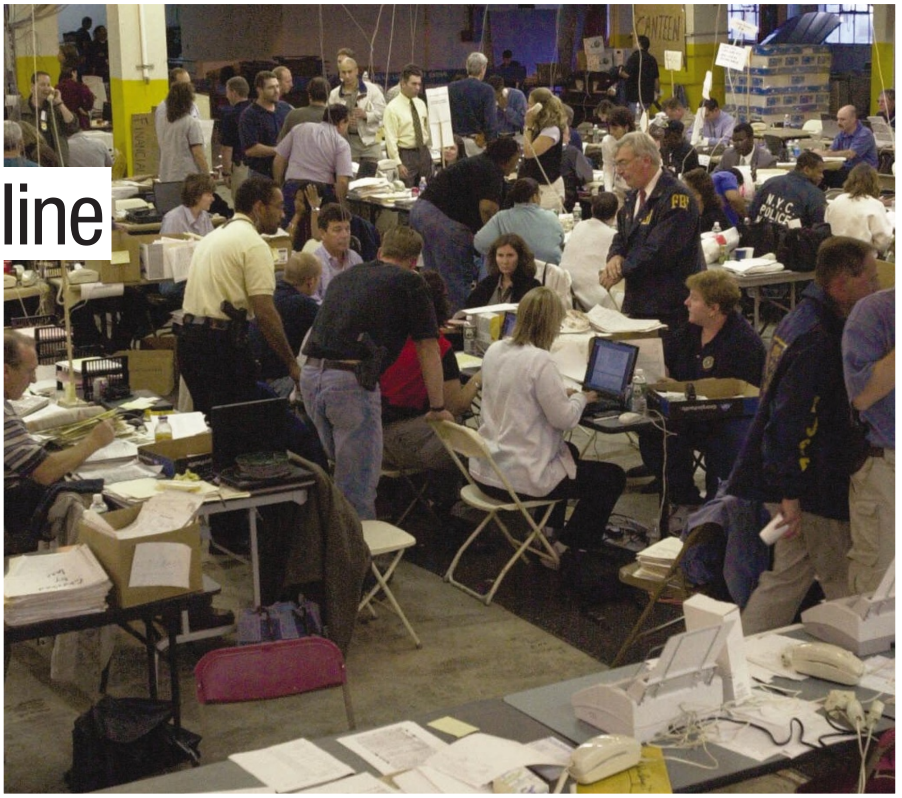
Cryptography on the front line

As the ‘war on terrorism’ unfolds, some politicians are calling for controls on the availability of encryption software. But many computer scientists claim such moves would play into the terrorists’ hands. David Adam reports.



AP

Crack team: the FBI is focused on terrorists — but could encrypted messages hamper its efforts?

Bankers, shoppers and other Internet users now have access to standards of privacy previously only available to the military. Off-the-shelf encryption software is effectively unbreakable — even by the massed computing power of organizations such as the US National Security Agency and the Federal Bureau of Investigation (FBI). Put that power in the hands of a terrorist network, and the potential for harm is all too obvious.

No surprise, then, that in the wake of the terrorist atrocities in New York and Washington, attention has focused on the ability of individuals to communicate securely over the Internet through encrypted e-mails. Although there is little evidence that those behind the attacks used such coded messages, some politicians are already calling for stronger controls on encryption software.

In a speech just days after the attacks, Republican Senator Judd Gregg of New Hampshire called for the US government to be given back-door access into all encryption software. Britain’s Foreign Secretary, Jack Straw, has also entered the fray, dismissing those who have fought against such moves in the past as “naive”. And on 6 October, the Dutch government announced that, as part of its counter-terrorism action plan, it intends to regulate the use of cryptography.

Coded warning

The events of 11 September had an immediate impact on public opinion — a poll conducted two days later indicated that 72% of Americans believed that anti-encryption laws would help to prevent repeat attacks.

But most experts on computer security argue that restrictions on encryption software would be expensive and impractical. Worse, they say that the net result would be to undermine the security of legitimate Internet users — rendering government and business more vulnerable to cyber-attack. But given the public statements of politicians such as Gregg and Straw, computer scientists are preparing for a reprise of the debate over privacy and security that they thought they had won in the 1990s.

“We’ve been through these arguments before, but legislators seem to have short memories,” says Bruce Schneier, chief technical officer at Counterpane Internet Security, a company based in Cupertino, California, that provides computer security services. “Limits on encryption and systems that ensure governments have access to encrypted messages will do little to thwart terrorist activities,” he argues. “At the same time they will significantly reduce the security of our own critical infrastructure.” (see Commentary, page 773.)

Encryption software uses mathematical algorithms both to scramble the contents of e-mails, by reordering the underlying data, and to decipher the encoded version. The algorithms are activated — and so protected — by numerical ‘keys’ typically containing 10 or more digits. One set of keys is widely circulated, and these are used to encrypt messages. But individual users also have private keys, which are used to decode messages. The algorithms and their mathematical relationships with the keys are too complex for security agencies to crack, so access to the private key is in practice the only way to read an encoded message.

Intelligence and law-enforcement chiefs have long been concerned about the potential misuse of such programs. Indeed, former FBI director Louis Freeh in the late 1990s warned repeatedly that terrorists could be using encryption software to plan their actions, and he urged the US Congress to approve restrictions on its use and distribution.

Added restrictions

But Schneier claims it is impossible to limit the spread of cryptography. "Cryptography is mathematics and you can't ban mathematics," he says. There are almost 1,000 software products that use cryptography, available in more than 100 countries. "You would have to ban them in every country and even then it won't be enough, as any terrorist organization with a modicum of skill can write its own cryptography software," he says.

Blanket restrictions on the use of encryption might also impede the use of computers and the Internet in activities such as online banking and shopping — which rely on encryption for security. A degree of disruption to e-commerce may seem a small price to pay for greater security, but cryptography systems also protect vital safety systems, such as the computers used in air-traffic control. "Restrictions are not possible from a practical point of view," argues Matt Blaze, a principal research scientist with AT&T Laboratories in Florham Park, New Jersey.

GETTY IMAGES

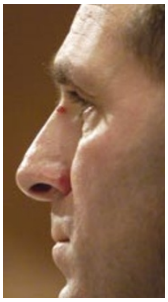
Clampdown: Louis Freeh (right) and Jack Straw want tighter curbs.

If governments cannot crack encrypted e-mails and they are unable to stop people using them, what options do they have? One is to force manufacturers to introduce 'back doors' into their encryption software, allowing the content of encrypted messages to be monitored routinely. This can be achieved by a system known as key escrow, in which copies of all private keys are handed over to a third party and can be accessed on demand by government security agencies.

The arguments for and against key escrow raged through the 1990s. Agencies such as the FBI argued that it would allow secure monitoring of communications with little disruption to normal Internet use. Civil-liberties groups campaigned against key escrow on privacy grounds, whereas computer scientists concentrated on practical flaws. Researchers in the field say that it is currently impossible to build a system that is secure enough to hold all of the private keys and guarantee that they could not be accessed by those intent on committing fraud or wreaking cyber-havoc. Particularly daunting are the human factors — ensuring that individuals working for the key-holding organizations cannot be bribed or otherwise manipulated into releasing keys.

"It's all very well protecting bars of gold because at least you can see if they're gone in the morning," says Richard Clayton, who works in the computer security group at the University of Cambridge. "But when you're talking about lots of numbers hidden on behalf of people and you can't even tell if they've been stolen, then you're talking about needing a very secure system indeed. We're just not capable of building such systems." Schneier agrees: "Stockpiling keys in one place over an extended time period is a huge risk just waiting for attack or abuse."

Another problem with key escrow is that there is little commercial demand for encryption software that can be accessed at will by a third party — even in the name of national security. "It's not easy to demand that individuals use designated software," says Wenbo Mao, a researcher in the mathematics, cryptography and security group at Hewlett Packard's UK laboratories in Bristol. "There is no market demand for it." Computer security experts are concerned that legislation enforcing key escrow would make legitimate computer users wary of using encryption technology — rendering their systems more vulnerable to attack.



With little incentive for software manufacturers to develop reliable key-escrow technology, the task falls to government agencies, which traditionally have kept this kind of research classified. But this approach is a problem, argues Mao — users have low confidence in a product that has not been subjected to widespread attempts to crack its codes. Indeed, the US government in the mid-1990s abandoned attempts to introduce its own key-escrow scheme, based on a system known as 'Clipper', after Blaze at AT&T exposed flaws soon after it was released. "Government-certified systems developed behind closed doors would be a potential disaster," agrees Brian Gladman, a computer security consultant who formerly served as secure systems director with Britain's Ministry of Defence.

Computer scientists thought that they had won these arguments — but now the world has been thrown into conflict, they are not so sure. "If encryption is used in issues such as terrorism, and there is no legal way that law enforcement has access, then that has to be an issue," says a spokeswoman for the British government's National Criminal Intelligence Service.

Britain, in fact, last year passed a law that computer security experts point to as an example of the sort of legislation that might be proposed elsewhere in the current climate. The Regulation of Investigatory Powers Act, championed by Straw when he was home secretary, gives police wide-ranging powers to intercept e-mail traffic, and also allows them to force individuals to surrender their private decryption keys. Refusing to comply, or revealing that you have been asked to surrender your keys, can be punished with up to two years' imprisonment.

AP

Summing up: Bruce Schneier urges governments to focus on improving computer security.

Key questions

These powers have not yet been invoked, so the impact of the law cannot be assessed. One problem is that the police must first show that seized private keys can be held securely. The scale of security needed for this more limited number of keys — which would not make such a tempting target — is not the same as that required for a full key-escrow system. But developing an appropriate system is still not easy. The British government admits that practicalities remain to be worked out, but says that it hopes to implement the law by the end of the year.

Given this, many computer scientists argue that the focus should not be on restricting the use of encryption, but on encouraging the development of stronger security systems to protect computer infrastructure vital for national and economic security.

To this end, President George W. Bush on 9 October appointed Richard Clarke, a former member of the National Security Council, to the post of special White House adviser for cyberspace security. "America built cyberspace and now it must defend cyberspace," Clarke said, in accepting the position.

Clarke's position on cryptography remains unclear. But even if he doesn't reopen the debate on encryption, other politicians and officials are determined to do so. Computer scientists who oppose such moves, it seems, will be forced to do battle once again. ■

David Adam is a news and features writer for *Nature*.