Detica

CHATHAM HOUSE

Terrorism, radicalisation and the Internet

Report of a private roundtable discussion on 22 July 2008

Terrorism, radicalisation and the Internet

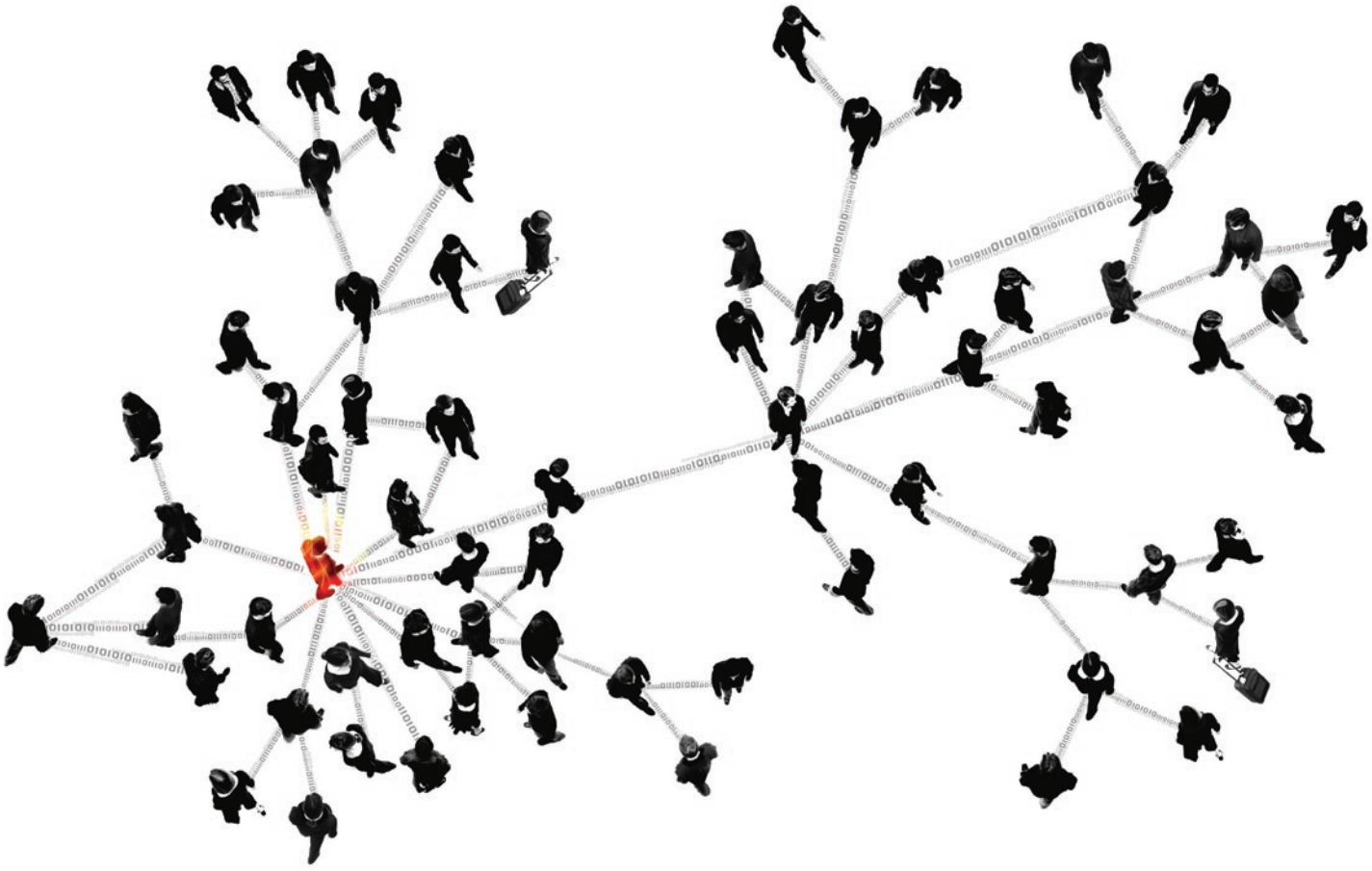
Report of a private roundtable discussion meeting

Dr Paul Cornish, Chatham House, 31 July 2008

This paper is an informal summary of a private roundtable discussion held on 22 July 2008 under the title 'Terrorism, radicalisation and the Internet'. The meeting was held under the Chatham House Rule. This paper is not a verbatim transcript of discussion and does not necessarily reflect the views of any person present at the meeting.

The meeting began with the presentation of a short paper in which three questions were posed:

1. What role does the Internet really play in radicalisation and can we identify the 'digital footprint' of such activity?
2. Should UK Government's PREVENT policies focus on disrupting the online channel, or on providing credible alternative messages?
3. How can the Internet be used more effectively to PURSUE extremists and those who radicalise?



What role does the Internet really play in radicalisation and can we identify the 'digital footprint' of such activity?

The concern with radicalisation is that it can result in exaggerated, dramatic and violent behavioural changes. Can use of the Internet give rise to such effects? Recent incidents in Bristol and Exeter suggest that the Internet did indeed have a role. But it is important not to exaggerate the significance of the Internet; if the Internet can have a radicalising effect, then it is only one of several conceivable sources of radicalisation, including educational institutions, working environments, faith-based organisations, prisons and even families. It is important, therefore, to establish the relative significance of the Internet as one among many possible paths towards, or tools for radicalisation.

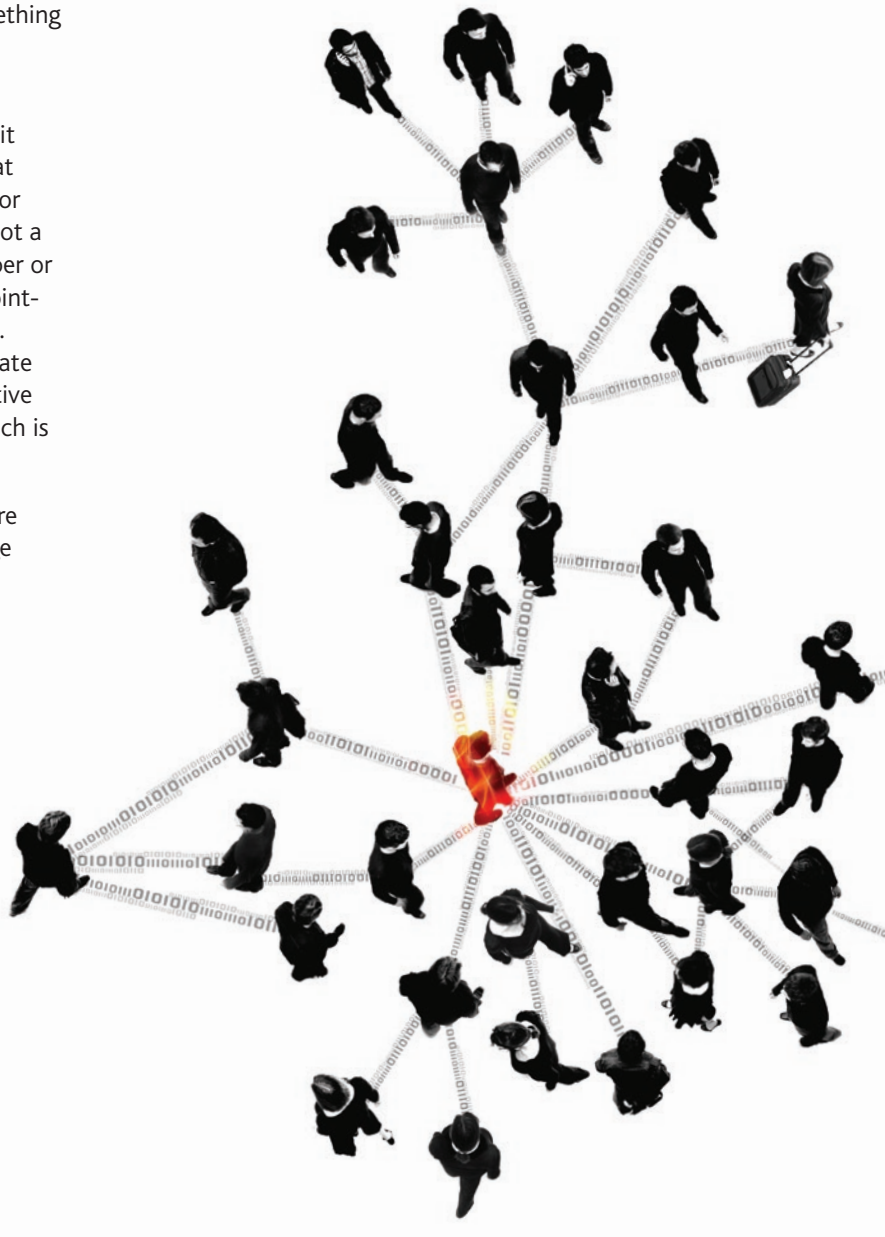
If the Internet does have a role in radicalisation, the next challenge is to know how the Internet can have such an effect. What is the balance of significance between *message* and *medium?* In other words, is the Internet merely a vehicle for a radicalisation process which is standard to all sources of radicalisation (universities, prisons etc.), or is there something distinctive and unique about the Internet as a tool for radicalisation?

One central feature of the Internet, for example, is that it is (or can be) to a considerable extent anonymous, yet at the same time can become a deeply personal medium for the exchange of information and ideas. The Internet is not a passive general information medium, such as a newspaper or a television broadcast. Neither is it an active, private, point-to-point communications service such as the telephone. The Internet offers a combination of these things: a private (often so private as to be furtive) means for the interactive assimilation of information and ideas from a source which is nevertheless largely anonymous.

The 'digital footprint' is not new; it has been a key feature in many recent prosecutions. Nevertheless, the challenge of identifying the 'digital footprint' of Internet-based radicalisation invites discussion as to the very nature of the Internet.

A mechanistic view of the Internet might be that it is a technological construct "where things happen". As such, it should be possible objectively to identify sequences of cause and effect, through the use of forensic and other investigation techniques, for example. A more dynamic view of the Internet, on the other hand, might see it as an organism which continues to develop and which, as it does so, will alter "the DNA of the human race". By this view, linear analyses of cause and effect will be difficult, and possibly misleading; the Internet is more of a subjective experience than an objective phenomenon, and it will be a problem to identify clearly the 'digital footprint' of any deviant or criminal activity since we – the 'observers' – are inextricably bound up in such activity.

Another useful view of the Internet is that it is simply chaotic; an example of Horst Rittel's 'wicked problem', where a traditional, linear problem-solving approach is inappropriate because the definition (and understanding) of the problem evolves as solutions to it are considered and implemented. Rittel and his colleague Melvin Webber described a 'wicked problem' as "messy, circular, and aggressive".



Should UK Government's PREVENT policies focus on disrupting the online channel, or on providing credible alternative messages?

In the words of one discussant, this question was something of a 'no-brainer' – it is clear that both approaches must be worked simultaneously. There are legal grounds for the disruption and disabling of certain Internet activity, and for more elaborate practices such as the infiltration of Internet chat rooms, and the use of these 'venues' for the purposes of counter-radicalisation. There are broader questions to ask, however, concerning the merits of Internet disruption. Analysis might show, for example, that well-intentioned public policy decisions and messages can inadvertently worsen the situation by contributing to a climate conducive to radicalisation, perhaps more so than any Internet chat room. And disruption of chat room activity might do little more than address the very late symptoms of much deeper problems in society. PREVENT policies should therefore address wider and deeper causes of radicalisation, and should also offer a feedback loop through which public policy can be subjected to critical appraisal. One benefit of such self criticism might be to understand the limitations of a traditional 'security' or 'defence' mindset when addressing the problem of radicalisation. A broader and more imaginative approach might be preferable, whereby knowledge and expertise can be drawn from a variety of disciplines such as sociology and social psychology in order to better understand the dynamics at work.

The need to provide 'credible alternative messages' is clear enough. The Research and Information Communications Unit (RICU) was established in 2007 with the remit to counter and undermine the 'single narrative' propagated by al-Qaeda and other extremist organisations. But this is not a simple task; these organisations are often highly expert and agile users of the Internet and other media, well aware that propaganda requires constant and careful management if it is to succeed. Furthermore, the popular narrative of radical Islamist organisations is largely that of a defensive jihad; a relatively simple message and in many quarters a very persuasive one. The most obvious counter-narrative to *defence* is *attack*, but this is unlikely to find much support among western liberal polities and would in any case merely validate the radical narrative. Western governments might, with reason, opt for a counter-narrative of prevention and denial of terrorist success; "terrorism might persist, but it will never succeed against us". Yet this is a largely passive position which does little to seize the initiative or to inspire confidence in a public which perceives itself to be vulnerable, and still less to deflate the narrative of terrorist and radical groups. Rather than a *counter*-narrative, what is required is a more activist *alternative* narrative, one which projects the attractions and strengths of western liberal society, through such ideas as democracy, rights and liberty.

Liberal society can, however, be curiously reticent about the ideas upon which it is founded, and can suffer from the morbid fear that the projection of those ideas would amount to illiberal proselytising.

Another 'credible alternative' message could lie in the notion of community. There is already a good deal of interest in the ways in which the Internet can be used to undermine the cohesiveness of local communities. But can the Internet also be used constructively; to help develop a benign spirit of community? This question invites thought as to what is meant by community and whether it is reasonable or proper to see the concept of community as something manipulable. 'Community' is a value-laden term, in that those communities which embody certain values and morés are regarded as politically, legally and morally more virtuous than others. This is therefore an implicit challenge to government; to express a preference as to which communities are acceptable to western liberal society, and which are not. But to meet that challenge governments must first be willing to project the 'activist alternative narrative' described above.

If it can be argued that the challenge of the Internet is (or should be) less to do with technology and more a matter of social norms and attitudes, and the cohesion of communities, then it has to be asked how a community can be bound together (or, indeed, be said to exist at all) when it is to a considerable extent an anonymous community, as well as being global and virtual. If the bases of community are identity and cohesion (physical or otherwise), then the antitheses of identity are anonymity and dispersion.

There might be merit in standing back from the problem in order to avoid an excessive and exclusive focus on the Internet. Open source material in a wide variety of media should also be examined in order to identify broad issues and trends both in society and among its critics. How well do we know and understand certain parts of UK society? What else can be done to understand public sentiment and feeling in some sections of society, and can technology assist in this 'soft' area? And if so, how can the effectiveness of such activities be measured?

How can the Internet be used more effectively to PURSUE extremists and those who radicalise?

For some time the PURSUE strand of CONTEST has been the main focus of concern regarding radicalisation and terrorist use of the Internet, arguably at the expense of PREVENT, PROTECT and PREPARE. The approach taken under PURSUE was also deliberately passive, following the argument that if the Internet could be left ostensibly undisturbed then it would be more likely to be regarded by criminal and terrorist organisations as a safe medium and more susceptible, therefore, to effective monitoring. By this argument, overt attempts to infiltrate the Internet would simply result in communications and other activity of concern becoming progressively more covert and difficult to track. The approach was broadly similar to that applied to the presence and activity of exiled extremists in north London in the 1990s, for which French critics coined the term 'Londonistan'.

There is an increasingly convincing argument for a more activist approach to be taken to the Internet and cybersecurity more broadly. Much of this reinvigorated approach is now being taken forward under the PREVENT strand, where a community-based mindset can be encouraged. Various activities could, however, be considered under the PURSUE strand, although a loose collection of disconnected responses will be no substitute for a fully co-ordinated strategy. Online filtering products, for example, proved to be effective when dealing with Internet-based paedophile activity, and might offer useful lessons for PURSUE. If anonymity is a central feature of the Internet, and a major impediment to security policy, then some consideration might also be given to online authentication of users' identity. A significant difficulty with authentication of identity, however, is that it would fuel the claim that a "surveillance society" is being constructed and could result in certain communities and sections feeling stigmatised and alienated. This in turn prompts discussion as to whether identity is indeed the most useful focus, and whether the idea of harm (broadly defined) might be a more valuable (and neutral) reference point.

In order to ensure that policy is focused as closely and effectively as possible, it should also be considered whether recruitment precedes radicalisation, or vice versa. Some are unequivocal in the view that recruitment must come first. But this is something of a circular problem since, presumably, a well-targeted radical statement could be a significant asset in recruitment. Rather than descend into this possibly insoluble argument, it might be more constructive to focus, first on the manner in which the Internet is used, and second on the sophistication and scale of the user.

Thus, a distinction could be drawn between the use of the Internet as a means of communication, and its use as a means to disseminate a recruiting (or radicalising) message. Equally, it should be possible to distinguish between the decision by one or a few individuals to undertake violent action for whatever reason, and the activity of a complex organisation gearing itself for an attack. Only the latter should be understood to be a strategic threat, and therefore of high-level national security concern.

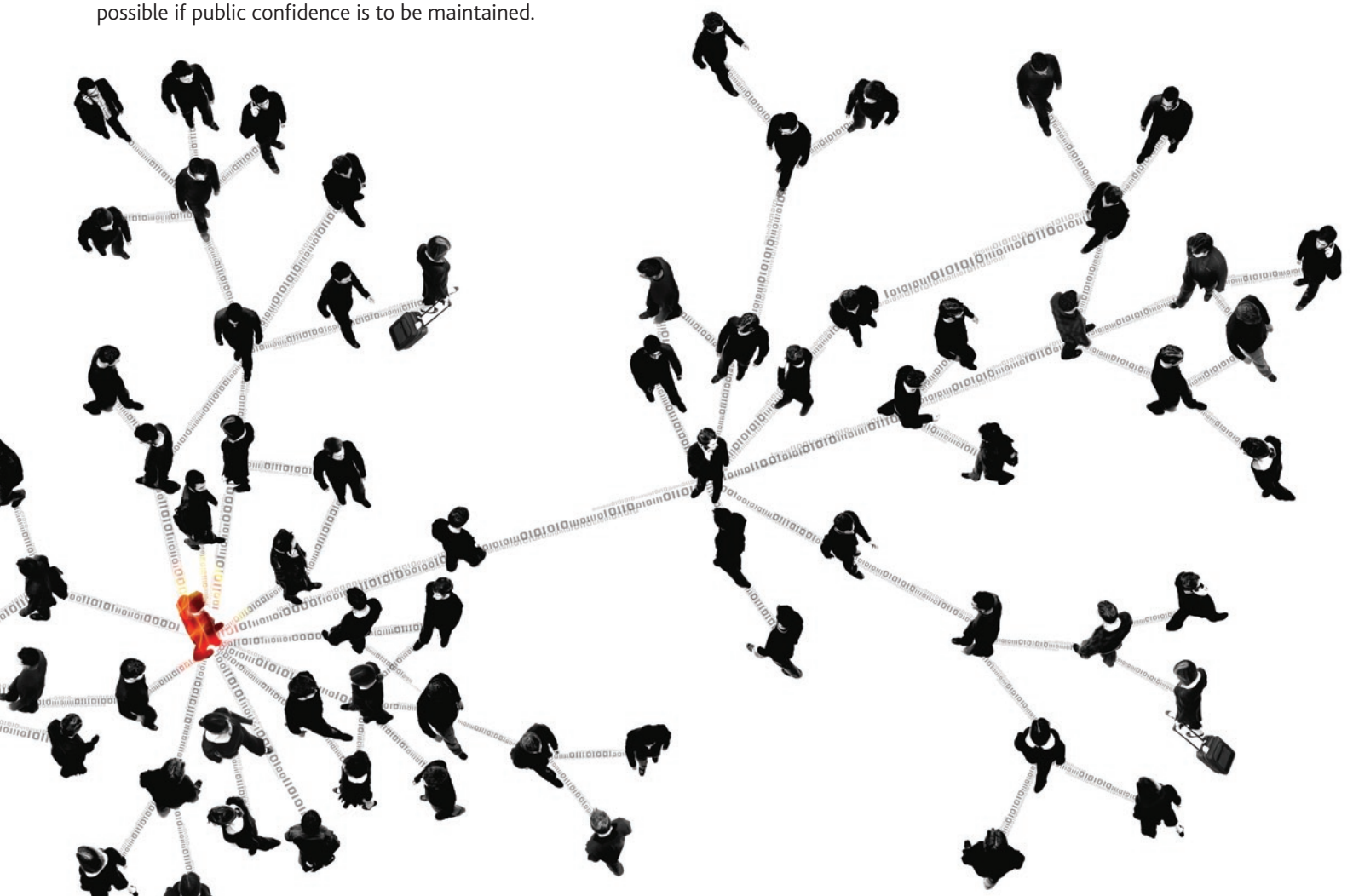
There can be a tendency to lose a sense of proportion and apply worst-case analysis to all radical activity on the Internet, even that which is little more than mischief-making. Equally, there can be an enervating tendency to assume that the adversary has all the initiative, all of the time, with the result that self-confidence is lost and defeatism takes hold. Western societies might indeed be engaged in an enduring ideological conflict with al Qaeda and similar organisations or movements, and it might well be the case that the radical narrative is both very persuasive as a recruitment device and unusually difficult to undermine. But it does not follow that western societies must also be at a technological disadvantage. Precisely the opposite is the case: western societies have a far better track record than al Qaeda in developing and deploying technology. But caution is needed here. It is because western societies have a technological lead that al Qaeda and similar organisations resort to opportunistic and parasitic behaviour. Western governments should therefore not be too open about the technologies and practices available to them, since to do so might simply persuade adversaries to adopt more covert methods. There are more straightforward grounds for confidence in the matter of recruitment: western societies are, after all, very experienced in recruiting young people into public service.

Conclusion

As with a number of issues – such as Chemical, Biological, Radiological or Nuclear proliferation, border security and policing – the Internet cuts across all four strands of CONTEST. The problem of the Internet cannot be comprehensively explored, and its potential fully exploited, in any one strand of the strategy. There is a strong case, therefore, for a more closely co-ordinated approach to the Internet in which the requirements of each strand are fully met, and opportunities fully developed. Co-ordination and strategic vision are essential; a "pin-prick" approach to the Internet – either within a specific strand or across CONTEST generally – is likely only to exhaust resources, without achieving the fullest possible effect.

Resources are limited, as in any area of public policy. But it is proper to ask, not only whether government-led activity is adequately funded, but also whether the relationship between government and industry is resourced to the level needed, in the form of funding for research, technology, development and procurement. It should not be assumed that success in any strand of CONTEST, or generally, can be achieved exclusively by government. The involvement of industry will be especially important, for two reasons. First, industry has developed a great deal of experience working with government in areas such as the policing of paedophile activity, where useful parallels might be drawn. Second, it will be essential to adopt as open and collaborative a model as possible if public confidence is to be maintained.

There is also an argument, finally, to suggest that the national level – however rich in collaboration between government, industry and others such as policy research institutes – is insufficient. Regional and international collaboration between security authorities and agencies will be essential. The most obvious case for such collaboration might be within Europe. But should the EU become a focus for inter-governmental policy co-ordination, or would it introduce a complex and bureaucratic model of policy making and activity where something lighter and more responsive would be preferred?



The Detica-Chatham House research project

The digital revolution has transformed the world around us but it has also created a new front line: where those who threaten our safety and way of life are exploiting the technology to an extent greater than ever before to facilitate or commit acts of terrorism or serious crimes. However, do we too have an opportunity to use this digital revolution? To better understand and anticipate the nature of the crimes and the criminals, to improve protection against malicious activity whatever the source, to prevent and deter malicious activity, and to pursue and take action against them? Only if we significantly change our thinking.

Detica and Chatham House have recently started a major policy analysis project, which is seeking a better understanding of how the nature of threats is changing and how to respond to the security challenges on the new front line. The project is divided into four modules:

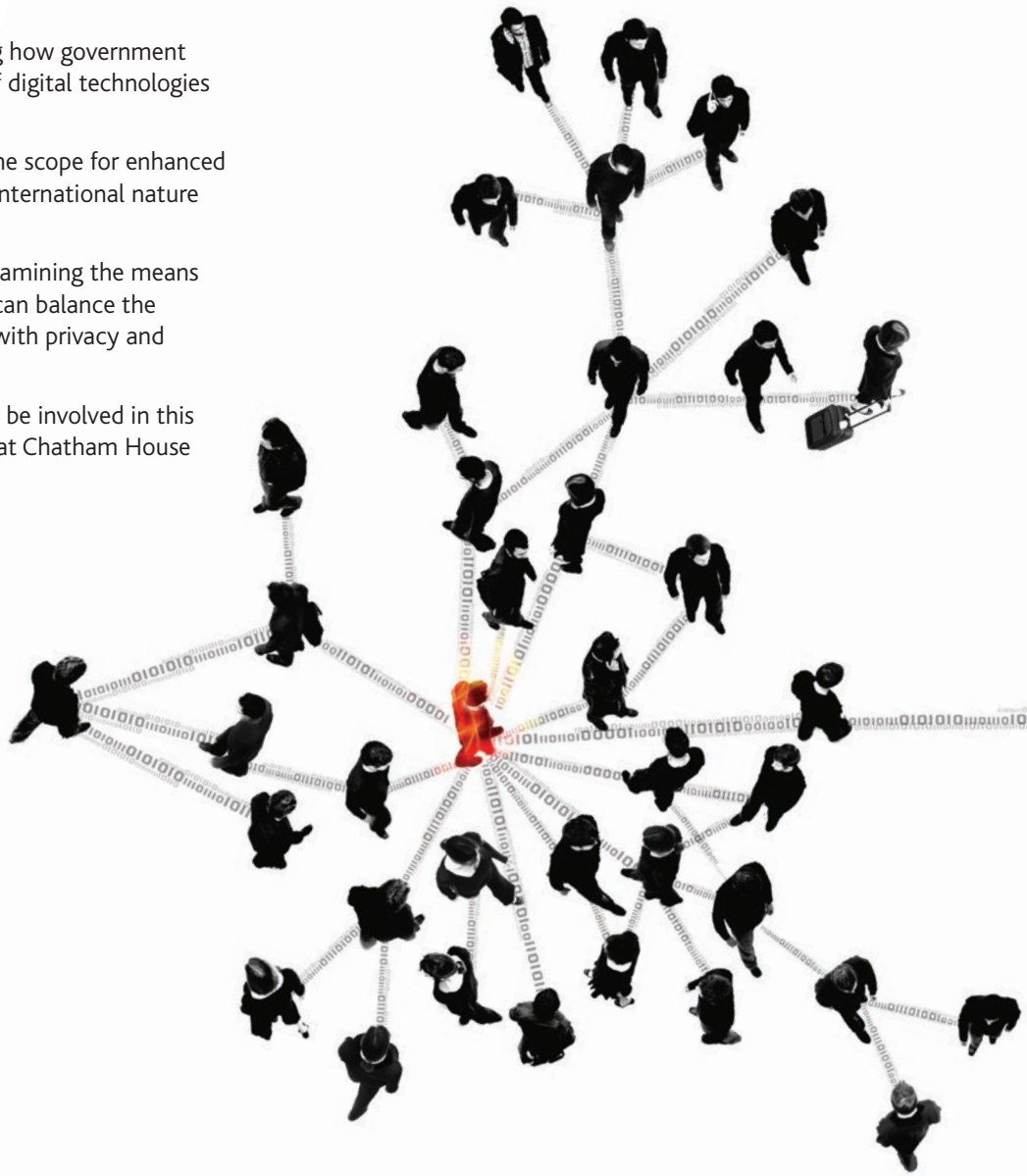
- Defining the threat: identifying the central features of the threat and examining innovative methodologies for analysis and response.
- Policy for the new front line: examining how government should respond to the increasing use of digital technologies for malign purposes.
- International collaboration: assessing the scope for enhanced multilateral co-operation to meet the international nature of this security challenge.
- Privacy, liberty, security and the law: examining the means by which a liberal, democratic society can balance the demands for security and surveillance with privacy and liberty.

If you would like to know more about or be involved in this research please contact Dr Paul Cornish at Chatham House (pcornish@chathamhouse.org.uk)

Detica roundtables

Detica hosts strategic roundtable discussions throughout the year. Many are "by invitation only" and attract senior decision makers and policy advisers across Government.

If you would like to find out more about future events or suggest themes for debate please contact Nick Wilding at Detica (nick.wilding@detica.com).



About Detica

Crime, border security, terrorism, identity fraud and defence are among the national issues that most consistently concern the public. Individuals want to go about their lives freely and with confidence. Among the many tools available to our clients, information can give them the vital edge to protect our society and way of life. Yet, the increasingly sophisticated methods used by criminals and extremists present an extraordinary challenge: how can the public and other vital national interests continue to be protected when the complexity of information is exploding?

Since 1971, Detica has been trusted by government clients in the UK, US, and by other international partners to provide meaningful insight and develop innovative technologies to solve challenges like these. We focus on the critically important areas of intelligence, security, risk and resilience "when information matters most" to help protect millions of people.

From strategy and analysis to training and equipment, we provide specialist consultancy, technology and managed services in the areas of:

- **Crime** – helping clients to reduce the harm of serious, organised and transnational crime.
- **Homeland security** – helping clients to protect borders and counter terrorism.
- **Resilience** – helping clients to understand and respond to emergencies, protect the critical national infrastructure, and deliver efficient, secure services.
- **Defence** – training, equipping and supporting the armed forces with specialist operational capabilities.

Detica

Find out more:

If you require further information please contact:

Detica Limited
Surrey Research Park
Guildford
Surrey GU2 7YP
UK

T +44 (0)1483 816000

thenewfrontline@detica.com

www.detica.com