Cyberspace and the National Security of the United Kingdom

Threats and Responses

A Chatham House Report

Paul Cornish, Rex Hughes and David Livingstone

CHATHAM HOUSE

www.chathamhouse.org.uk

Cyberspace and the National Security of the United Kingdom

Threats and Responses

A Chatham House Report

Paul Cornish, Rex Hughes and David Livingstone

March 2009

CHATHAM HOUSE

www.chathamhouse.org.uk

Chatham House has been the home of the Royal Institute of International Affairs for over eight decades. Our mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all.

Detica specialises in collecting, managing and exploiting information to reveal actionable intelligence. We use this capability to help government and commercial clients reveal intelligence, maintain security and strengthen resilience in today's complex operating environment. Detica delivers projects of significant scale across government and commercial markets in the UK, US and continental Europe. Our principal clients are government agencies responsible for intelligence, security and resilience. We also assist civil government and commercial organisations with a critical national infrastructure remit.
www.detica.com

Chatham House (the Royal Institute of International Affairs) is an independent body which promotes the rigorous study of international questions and does not express opinion of its own. The opinions expressed in this publication are the responsibility of the authors.

Chatham House
10 St James's Square
London, SW1Y 4LE
T: +44 (0) 20 7957 5700
F: +44 (0) 20 7957 5710
www.chathamhouse.org.uk

Charity Registration No. 208223

ISBN 978 1 86203 215 6
A catalogue record for this title is available from the British Library

Designed and typeset by
Soapbox Communications Limited,
www.soapboxcommunications.co.uk

Printed and bound in Great Britain by Latimer Trend and Co Ltd

The material selected for the printing of this report is Elemental Chlorine Free and has been sourced from sustainable forests. It has been manufactured by an ISO 14001 certified mill under EMAS.

Contents

About the Authors

Dr Paul Cornish holds the Carrington Chair in International Security at Chatham House, where he directs the International Security Programme. He was educated at the University of St Andrews, the London School of Economics, the Royal Military Academy Sandhurst and the University of Cambridge. He has served in the British Army and the Foreign and Commonwealth Office, has taught at the UK Joint Staff College and at the University of Cambridge, and was previously Director of the Centre for Defence Studies at King's College London. His research interests include European security and defence institutions, arms control and non-proliferation, counter-terrorism and domestic security.

Dr Rex Hughes is a Research Associate at the Cambridge-MIT Institute where he examines the global governance challenges of cybersecurity. He was educated at the Universities of Washington and Cambridge. He founded and directed the world's first multidisciplinary Internet Studies programme at the University of Washington. Working in partnership with IBM-Lotus, Dr Hughes led the development of iEnvoy, the first secure diplomat-to-diplomat Internet communications platform deployed by the US Department of State.

David Livingstone MBE DSC is the Managing Partner of Morgan Aquila LLP, which provides consultancy in business transformation in the anti-terrorism domain, focusing on the benefits derived from multi-agency integration. During 21 years in the Royal Navy he was variously a helicopter pilot, minesweeper captain and staff officer with the Flag Officer Naval Aviation. He is a graduate of the Army Staff College Camberley and a Fellow of the Royal Geographical Society. He has written a number of papers on counter-terrorism and resilience, and is a regular media commentator. Mr Livingstone is an Associate Fellow of the International Security Programme at Chatham House.

Preface

This report forms the first part of a major project on cybersecurity undertaken by Chatham House in conjunction with Detica Ltd. The project aims to engage government, private-sector, academic and other specialists in high-level analysis of cybersecurity challenges and responses.

Where cyberspace and national security are concerned, there is a disconnect between technology and public policy which this project seeks to bridge. Science and technology should be more closely informed by public policy, while a technologically informed political leadership should be better placed to meet the cybersecurity challenge. This project will provide a forum for constructive exchange in which the possibilities and limitations of technology can be fully explored, and in which the parameters of public policy-making can be more closely understood by those charged with developing the technological dimensions of security policy.

The project comprises a series of reports. This first report identifies the central features of the cybersecurity challenge and examines innovative methodologies for threat analysis and response. Future reports will address the specific demands of national cybersecurity policy, the requirement for international cooperation, and the balance to be struck between safety and security on the one hand, and privacy and liberty on the other.

Acknowledgments

The authors wish to thank all those who read and commented upon earlier versions of this report, and who attended study group meetings at Chatham House.

The views expressed in this document are those of the authors, who accept responsibility for any errors of fact or judgment.

March 2009
P.C., R.H., D.L.

Executive Summary

Cyberspace and the National Security of the United Kingdom provides a general overview of the problem of cybersecurity. The aim of the report is to inform debate and to make the case for a more coherent, comprehensive and anticipatory policy response, both nationally and internationally. In every area, society is becoming increasingly dependent upon information and communications technology (ICT). With dependency come exposure and vulnerability to misuse, criminality and even attack. Criminals and extremists are able to take advantage of the same 'global technological commons' upon which society is becoming so dependent. Cybersecurity has become a fast-moving and complex security challenge, one which requires a coordinated, agile and mutually reinforcing response from all those who benefit from the global ICT infrastructure.

After a brief introduction, Chapter 2, on cyberthreats, describes four domains of hostile activity and behaviour: state-sponsored cyberattacks, ideological and political extremism, serious and organized crime, and lower-level/individual crime. These domains are inter-linked. Hacking, for example, is a relatively low-level and disorganized activity, yet it can have very high-level consequences, and it also features prominently in other threat domains. Serious and organized criminal misuse of the global information infrastructure is increasing, in both quantitative and qualitative terms, and at considerable cost to the global economy. What is more, the Internet seems to fit the requirements of ideological and political extremists particularly well. Finally, it seems that the Internet is increasingly seen by some states and governments as a strategic asset to be exploited for the purposes of national security, and perhaps even as a battlefield where strategic conflicts can be fought. The report observes that it is not simply that increasing dependence on ICT creates vulnerabilities and opportunities to be exploited by the unscrupulous, but also that ICT has an increasingly important enabling function for serious and organized crime, ideological and political extremism, and possibly even state-sponsored aggression.

As a complex security challenge, cybersecurity cannot be explained sufficiently in terms of threat. In Chapter 3, on cybersecurity practices and principles, the report argues that cybersecurity amounts to a system-level challenge to society. A system-level response will be necessary so that the activities of different agencies and bodies complement each other and are mutually reinforcing, rather than conflicting. Yet society does not respond as a coherent system; different stakeholders remain focused on their narrow interests and as a result the cybersecurity response is dispersed, uncoordinated and inefficient. Current practices (such as computer and network security, information security and assurance, and the protection of critical national infrastructure) must be informed and energized by a set of strategic and operational-level principles, including governance, inclusiveness, agility and risk management.

In Chapter 4, which looks at the challenge of building a national cybersecurity regime, the report draws on recent experience in the United Kingdom to show how a coherent framework for cybersecurity policy can be developed, in which 'bottom-up' and 'top-down' approaches can be integrated, and in which a more systemic approach to cybersecurity becomes feasible. A national cybersecurity regime should include (yet not direct) a wide variety of actors, agencies and stakeholders, and must be sufficiently agile (yet without losing focus) to meet a rapidly evolving and transforming security challenge.

In summary, the report makes a number of observations and recommendations for further research and analysis:

- Cybersecurity is not exclusively a military problem. The language and organizing concepts of cybersecurity can often seem to be military in derivation; 'threat', 'aggression', 'attack', 'defence' being among the more familiar terms. But cybersecurity is a challenge to society as a whole and requires a broad, cooperative multi-agency response.

- Society is becoming ever more dependent on the global ICT infrastructure. With dependence comes vulnerability to those who would exploit features of this infrastructure to prey on society for their own nefarious ends.
- Yet when hackers, criminals and extremists use ICT against society, they too become ICT-dependent and therefore vulnerable to surveillance and disruption by law enforcement and other legitimate agencies.
- Business process analysis provides a basis for action against cyberdependent adversaries.
- Proportionality is essential. Cybersecurity is a serious, structural challenge. But assessment of the character and scale of cyberthreats can be exaggerated. Careful analysis of cyberthreats (ideally cross-governmentally) is necessary in order to ensure a proportionate and cost-effective response.
- Efforts should be made to improve the relationship between the worlds of security policy and technology. Specialists in cybertechnology – the so-called 'technorati' – should be given a more central and formative role in policy.
- Because cybersecurity affects all sectors and levels of society, there are fundamental choices to be made as to how responsibility for it should be distributed between the private, commercial and governmental domains. In the sphere of public policy specifically, decisions must be made over which government department should be charged with developing and articulating a policy, and how different aspects of policy should be apportioned among agencies.

1 Introduction

'Cyberspace', 'cybersecurity' and other related expressions are widely used as though their meaning were clear and beyond debate. The reality, however, is that these terms mask a range of untested assumptions and unanswered questions, posing a serious difficulty for policy-makers and those responsible for national safety and security. Cybersecurity (security in and from cyberspace) is widely regarded as an urgent and high-level problem which cannot be ignored. But the precise nature of this problem is not well defined. This combination of intuition and uncertainty (mixed with pessimism) can subvert analysis, encouraging a shift in the direction of worst-case assessment and a tendency to focus policy (and expenditure) almost exclusively on high-impact/low-probability events. The stakes are, of course, very high and catastrophe is possible even if the likelihood is low. But insurance-style arguments of this sort risk turning policy-making into something reactive, uncritical and disproportionate, with any and every imaginable crisis somehow given 'priority' status.

'With dependence come exposure and vulnerability, and an ever-widening array of opportunities for the unscrupulous to exploit'

Neither worst-case analysis nor its opposite, complacency, offers a good basis for policy-making, yet in cybersecurity more considered approaches are difficult to achieve. The information and communications technology (ICT) which is increasingly being exploited by miscreants, ranging from political extremists to organized criminal groups to individual hackers, is essentially indistinguishable from that used for entirely innocent and legitimate purposes. And these legitimate uses are often not 'optional extras', which society might set aside for reasons of safety and security.

Since the introduction of the integrated circuit in the 1950s, the world economy has grown increasingly dependent on a digital information infrastructure. In 2009 it is difficult to imagine a major business or organization that does not rely on advanced ICT. Industries ranging from railways to retailing all depend on high-performance ICT systems to maintain essential business communications with both customers and suppliers. In the financial sector, business worth hundreds of billions of dollars is transacted daily via global data networks, public and private. In the public sector vital institutions also rely on cyber-based systems to deliver critical health, education and social services. Society's dependence on ICT systems and networks seems likely only to deepen; the advent of 'cloud computing' will mean that digital technology will 'penetrate every nook and cranny of the economy and of society.'[1] It is no exaggeration, therefore, to say that the global economy is now dependent upon a broadband-enabled cyberknowledge complex. With dependence come exposure and vulnerability, and an ever-widening array of opportunities for the unscrupulous to exploit.

Society's dependence on ICT is exacerbated by the increasing interdependency of information systems, making it difficult to know what repercussions failure in one part of the system will have in another. As dependence on this complex system increases, so too does society's vulnerability to misuse of it, and so too does the severity of the consequences of attack or system failure (which might, in practical terms, be indistinguishable). And as we have suggested, society is increasingly dependent – perhaps absolutely so – upon technology which adversaries themselves might use to attack.

In these circumstances, it is not easy to determine what should be protected, against whom and with what means. But the challenge of cybersecurity goes far deeper.

Cybersecurity is often described, explained and analysed within a traditional policy framework, where the language and organizing concepts are often military in derivation; 'threat', 'aggression', 'attack', 'defence' are among the more familiar terms. In some cases, it might be appropriate to analyse the problem in this way, and to act accordingly. But the application of orthodox security and defence thinking can too often result in cybersecurity being understood as something which intrudes from outside, which is 'done' by 'them' to 'us'. Yet the correlation between dependence and vulnerability gives an important indication that cybersecurity is a more challenging problem than this, one which might not be conducive to a linear analysis based on action and reaction, cause and effect. Indeed, cybersecurity is probably better understood as a *complex* problem, one which is characterized by uncertainty and non-linearity, which is dynamic and continually evolving, and in which it can be difficult to establish clear causal relations and sharp dividing lines between subject and object.

The aim of this report is to provide an overview of the problem of cybersecurity, in order to inform the debate and to provide the basis for subsequent, more detailed analysis of national and international policy-making in this sphere. Although the report is written largely from a general security policy perspective, the authors argue that technical specialists – the so-called 'technorati' – should have a more central role in cybersecurity policy-making, if policy is to be as coherent and agile as it can be. Chapter 2 discusses threat, describing important 'domains' of cybersecurity activity and behaviour. In keeping with the claim that cybersecurity cannot be explained sufficiently in terms of threat, Chapter 3 – 'Cybersecurity: Practices and Principles' – begins by describing current initiatives and procedures in cybersecurity policy, in both the public and the private sectors. It then presents a set of strategic and operational-level principles to help shape cybersecurity policy-making and implementation. Using UK experience to illustrate the argument, Chapter 4 sets out a coherent framework for cybersecurity policy, in which 'bottom-up' and 'top-down' approaches can be integrated, and in which a systemic approach to cybersecurity can be developed.

2 Cyberthreats

The integrity of the global cyberknowledge complex is critical not only to the day-to-day functioning of the world economy, but also to the security and well-being of governments, organizations and people: public bodies can be attacked, commercial interests can be defrauded and individuals can be subject to a range of assaults. In the United Kingdom in 2007–08, by one account, approximately 830,000 businesses experienced an online or computer-related security incident, and in 2007 around 40 per cent of personal identity fraud – some 84,700 cases – took place online.[2] The first step in any analysis of cybersecurity must indeed be to chart the range of cyberthreats, by which we mean security challenges made either *via* or *to* ICT equipment and networks. An apparently straightforward, descriptive task, this can be a difficult undertaking, not least because these two broad categories of security challenge can overlap considerably. Microsoft, for example, has developed a data centre near Chicago which requires three electricity substations with a capacity of 198 megawatts – 'as much as a small aluminium smelter' – disruption of which could fall into both categories of attack just described.[3]

The transformation of the Internet from an elite research network to a mass communications medium has altered the global cyberthreat equation dramatically. The global ICT system can be exploited by a variety of illegitimate users and can even be used as a tool in state-level aggression. These activities can be organized along a spectrum running from lower-level, individual crime (e.g. hacking), to the behaviour of non-state actors and groups (i.e. criminals and terrorists), to plans orchestrated by governments. But it is important to note that while this spectrum of activities has merit as an organizational device, it is flawed analytically. These diverse users of the Internet do not fall into discrete camps, and least of all into a simple hierarchy of threats. Hacking, for example, can have uses in very serious organized crime; organized criminality can be linked to international terrorism; and terrorism can be used as a tool of state aggression. This point is made most strikingly in the late 'Bali bomber' Imam Samudra's prison autobiography, in which a section entitled 'Hacking, Why Not?' reportedly urges young Muslims to 'take the holy war into cyberspace by attacking U.S. computers, with the particular aim of committing credit card fraud', with which to fund the struggle against the US and its allies.[4] With that caveat in mind, this chapter discusses challenges to cybersecurity in terms of four cyberthreat domains: state-sponsored cyberattacks; ideological and political extremism; serious and organized crime; and lower-level/individual crime.

Cyberthreat domain no.1: state-sponsored cyberattacks

Interstate misuse of the cyberworld can begin at a relatively low level of technology. It would be a mistake to assume, however, that the significance of such attacks is commensurately low-key. In April 2008, for example, reports circulated of an attack against eight Internet sites operated by Radio Free Europe/Radio Liberty. In an orchestrated attempt to overwhelm the target sites, some 50,000 fake hits were recorded every second. This was scarcely the most sophisticated form of cyberoperation. Yet the source of the attack was alleged to be none other than 'Europe's longest-ruling dictator, Belarus's Aleksander Lukashenko', who reportedly wanted to limit media coverage of opposition protests against his regime.[5]

The RFE/RL case illustrates a recent trend in Internet misuse which is more systematic and which has consequences far more serious than the temporary jamming of radio broadcasts. In September 2000, Israeli hackers attacked and defaced websites owned by Hezbollah and the Palestinian National Authority. In the Palestinian response – tellingly described as a 'cyber holy war' – Israeli government and financial websites came under assault. In 2001, following a dispute over damage to US and Chinese aircraft in the South China Sea, both countries suffered a series of cyberattacks, and at one stage California's electricity grid was almost shut down. Neither government accepted responsibility for launching the operations, although both have reportedly conducted research into the viability and effect of cyberweapons.[6] More recently, the cyberattacks launched against Estonia in April and May 2007 have captured attention internationally. In a dispute over a Russian war memorial in Estonia, Estonian government and banking websites and Internet providers were the targets of Distributed Denial of Service (DDOS) attacks. These attacks – the so-called 'Clickskrieg' – were especially disabling for a country which held itself up as a pioneer of electronic government. There was some uncertainty as to who had orchestrated the attacks – was the culprit a 'flash mob' of Russian computer users,[7] or the Russian government itself? – although the Estonian authorities eventually prosecuted a lone hacker. One important lesson of the Estonian affair was that even very large organizations and government departments are vulnerable to disabling attacks of this sort, and the episode contributed to the decision to consolidate NATO's Co-operative Cyber Defence Centre of Excellence in Estonia.[8]

> ‘It is likely, if not certain, that cyberwarfare will be an increasingly important feature of conflict between states in years to come’

Drawing lessons from the long military tradition of electronic warfare, cyberoperations have also become a feature of conventional military attacks. In September 2007, for example, an Israeli air strike against a target in Syria was reportedly assisted by a parallel cyberattack against Syrian air defences, enabling non-stealthy Israeli aircraft to move into Syrian airspace without fear of detection and interdiction.[9] For one analyst, this was an indication of things to come: 'More and more often, cyber attacks on government servers signal a physical attack in the offing.'[10] This warning rang true within one year, during the Russo-Georgian conflict over South Ossetia in summer 2008. Described as 'the coming of age of a new dimension of warfare',[11] the conflict saw private computing power organized and coordinated in such a way as to have strategic effect on a national enemy. It is not clear that the Russian government was directly behind or formally approved the DDOS attacks on Georgia, but it seems likely that the attacks were at least officially not prevented. Although no serious long-term Georgian cyberdamage was reported, the coordinated attack showed an 'untapped potential for using the Internet to cause mass confusion for political gain.'[12]

It is likely, if not certain, that cyberwarfare will be an increasingly important feature of conflict between states in years to come.[13] Indeed, losses and gains made in cyberspace might be so decisive that the character of warfare could change fundamentally, as the physical and the territorial parameters of conflict give way to the virtual and the digital. Analysis clearly points in this direction. It is estimated that a large-scale DDOS attack against the United States, for example, could have devastating effect: if power and other services could be shut down for a period of three months the damage could be equivalent to '40 or 50 large hurricanes striking all at once.'[14] China's intentions and capabilities often feature prominently in analysis of this sort. According to a recent US Congress policy review panel, 'China is aggressively developing its power to wage cyber warfare and is now in a position to delay or disrupt the deployment of America's military forces around the world, potentially giving it the upper hand in any conflict.'[15] An increasing number of electronic 'intrusions' are reported to originate in China, although it is not entirely clear how far this activity is officially approved. China is thought to be allocating very significant resources to computer network operations (CNO), including computer network attack (CNA), computer network exploitation (CNE) and computer network defence (CND). By reducing vulnerability to countermeasures, CND would be a crucial feature of cyberdependent operations, and it is consistent with the view that the Chinese

People's Liberation Army would seek to achieve 'electromagnetic dominance' early in a conflict, and to maintain that advantage.[16]

If cybersecurity does become increasingly militarized, and if the Internet does become one more weapon in a 'state sponsored act of war,'[17] then a number of intriguing political, technological and ethical questions are raised. What is the best form of defence in cyberwarfare? What exactly are 'cyberweapons'? Are they weapons of war, combat aircraft and artillery guns? Is the Internet merely harmless technology, or is it to be regarded (like traditional weapons) as something which can be used to damage, destroy and kill, and to be regulated as such? Is it reasonable or useful to regard cyberweapons as equivalent in magnitude to 'weapons of mass destruction'?[18] And finally, how could the origin of a cyberattack and the identity of the perpetrator be ascertained?

Cyberthreat domain no. 2: ideological and political extremism

Terrorists and other extremists are known to make extensive use of the Internet. The number of extremist websites has increased at an enormous rate, from 'a handful in 2000 to several thousand today',[19] and by one account the Internet is becoming 'the most important meeting place for jihadis all over the world, to communicate, discuss, and share their views.'[20] So-called 'cyberterrorism' begins with hacking and lower-level criminality. Younis Tsouli, described as 'one of the most notorious cyberjihadists in the world,'[21] used hacking skills (in which he trained others) to break into and subvert computer networks in order to distribute video files of terrorist attacks, and to use the proceeds of common credit card fraud to set up jihadi websites.[22] By these means, Tsouli was to become 'the administrator of one of the most important extremist websites which facilitated contacts between thousands of individuals.'[23] Following his arrest and subsequent imprisonment, Tsouli's activities were described by a senior counter-terrorist official as 'the first virtual conspiracy to murder that we had seen', and as an important indication of the way extremists had become proficient at conducting operational-level planning on the Internet.[24]

The popularity of the Internet for ideological and political extremists can be explained in a number of ways. By origin, design and function, the Internet could scarcely be improved upon as a medium for extremist organization and activity. The origins of the Internet lie in the Cold War, and in the need to ensure redundancy in governmental and military communications systems in the event of a nuclear strike. It should be no surprise, therefore, that extremists are also attracted to a system which offers in-built resilience and virtual anonymity. They may also be attracted to a system which is relatively cost-free, and where the investments necessary to develop and maintain the global communications infrastructure have already been made – ironically by their enemies.[25] The Internet is an anarchic common ground – some might call it an ungoverned space – which extremists can exploit in unremarkable ways, just as society does, for such purposes as communication and information sharing.[26]

By design, the Internet is also especially suitable for use by organizations which are deliberately opaque in their structure and intention. Indeed, as organizations become more opaque and complex, so the value of the Internet increases accordingly, making it progressively more difficult to identify the organizations in question and to track their progress. In April 2007 a senior UK counter-terrorism police officer described the problem as one of dealing with 'networks within networks, connections within connections and links between individuals that cross local, national and international boundaries.'[27]

In functional terms, the Internet offers a number of useful services for extremists. In the first place, it is a medium for communications at various levels of obscurity; clear, encrypted and steganographic.[28] Executive orders can be transmitted by these means, operations can be planned and fund-raising campaigns organized. Through the use of discussion forums, bulletin boards, media groups, blogs and web postings, the Internet can also allow training and techniques – and even ideas – to be discussed interactively. Tactics and procedures can be improved through a process of rapid online evaluation, and doctrine and ideology can be subject to criticism. By this approach, something as uncompromising and determined as a terrorist campaign can give the impression (not least to potential recruits) of being inclusive and consensus-based.

As a versatile communications medium, the Internet lends itself to the production and distribution of propaganda. Extremist groups have always, of course, made heavy use of propaganda, in the form of printed publicity and, more recently, video recordings. The Internet makes this material vastly more accessible and reproducible, through passive web postings and interactive chat rooms. It can also give immortality to a propaganda message, ensuring that the words of an imprisoned or deceased radical leader remain as a source of inspiration. Finally, it can act as a propaganda library; a repository for religious, political and ideological literature, and for more prosaic instruction manuals and videos covering tactics and operational techniques.[29]

With instruction manuals so readily available, the Internet has become a place of teaching and instruction. Interactive tutorials can be offered, in a wide range of subjects from weapon handling through to the skills needed to write malicious code and sabotage computer networks.[30] Tactical and operational training can be conducted through simulators and even online computer games, including Massively Multiplayer Online Role-Playing Games (MMORPGs).[31] With all this activity, the Internet is often described as a 'virtual training camp' or 'open university' for extremists, where recruits can be prepared to the level necessary to mount a terrorist or insurgent attack, or selected to attend a live training camp such as those in Iraq and Pakistan.[32] For some, this is all by design – a distinct and deliberate feature of the global Islamist insurgency. In a May 2008 report by the US Senate, for example, Internet activity of this sort was described as a 'virtual extremist madrassa', part of a 'comprehensive, tightly controlled messaging campaign by al-Qaeda and like-minded extremists designed to spread their violent message.'[33]

Some analysts are more sceptical, however. Daniel Kimmage claims that the use of the Internet for these purposes is a matter of necessity, rather than choice. Extremists, he argues, have been 'impelled' to adopt a decentralized organization (and, by extension, online means of communication) because the global jihadist movement is in practice 'a chaotic amalgam of international terror cells and localized insurgencies that espouse loosely articulated common goals yet lack the organizational cohesion of a movement and face an unprecedented global security clampdown'. Kimmage sees the jihadists' use of electronic media as a function of weakness rather than strength, and argues that they are determined to impose more control and organization rather than less 'to mimic a "traditional" structure in order to boost credibility and facilitate message control.'[34] Others consider the 'virtual training camp' idea to be an exaggerated assessment of the capabilities of al-Qaeda and similar organizations. While it is certainly the case that virtual training and teaching do take place, they do not necessarily form part of a carefully constructed programme driven centrally by al-Qaeda. Instead, the Internet is better understood as a 'resource bank maintained and accessed largely by self-radicalized sympathizers', and more of a 'pre-school of jihad' than a university.[35]

There is generally more agreement, not least among government agencies, on the importance of the Internet for the indoctrination, recruitment and radicalization of extremists. The Dutch domestic intelligence service, for example, describes it as the 'turbocharger' of radicalization,[36] and in May 2007 the Saudi Interior Ministry claimed that the Internet was responsible for 80 per cent of the recruitment of youths for the jihad.[37] In the UK, security agencies are described as fighting a 'covert war in cyberspace against extremist Islamist Internet sites'.[38] Recruiting has become such an important feature of cyberextremism that one 'al-Qaeda jihadi Internet forum' has uploaded a 51-page manual entitled 'The Art of Recruitment', intended to show how individuals can be drawn in and eventually establish an active jihadi cell.[39] With so many resources available on the Internet, recruitment and radicalization are no longer simply a matter of 'organizational pull', but are also increasingly a matter of 'individual push' or self-recruitment and self-radicalization.[40]

Self-radicalization is an important and intriguing concept. Some extremist groups have advocated the establishment of disconnected, self-starting, independent terrorist cells, not linked directly to any network or hierarchy but able to carry out large-scale terrorist attacks. Abu Mus'ab al-Suri, author of *The Global Islamic Resistance Call*, is reported to have recommended that jihadist training should take place in 'every house, every quarter and every village'.[41] Out of this process the so-called 'home-grown terrorist' can develop; a combination of anonymity and violent potential which is a cause of concern for Western intelligence and counter-terrorist agencies. Self-radicalization also suggests that for extremists the Internet is both much more and, curiously, much less than a global communications network. It offers a way not only to proliferate but also to 'atomize' the extremist campaign;[42] the global jihad can be achieved, in other words, without the continued requirement for elaborate communications networks and a well-organized global command structure. Widely dispersed and self-radicalized jihadists are brought together in a 'global Islamic movement fighting to defend the global ummah, or community, from a common enemy.'[43] By this ingenious route, the extremist message is adopted and implemented by self-radicalized individuals who are then connected with each other, less through the infrastructure of command, control and communications than through a simple common cause.

Once radicalized and trained in this way, extremists can then find that the Internet continues to be useful as a weapon. In the clearest illustration of this trend, there are those extremists for whom it has become a 'battle space' in its own right; a territory in which a 'virtual jihad' can be fought. These individuals might contribute by commenting upon, reproducing and distributing the thoughts of terrorist leaders, by collecting and distributing open-source information useful to operational planners, and by taking part in more active measures such as hacking and 'denial of service' attacks: 'These self-appointed amplifiers of the violent Islamist message […] choose to advance the cause, not necessarily with guns but with propaganda.'[44] Others see the Internet as a more active weapon, enabling terrorists and insurgents to magnify the symbolic effect of their attacks.[45] Clearly, if the 'infosphere' is indeed an 'ungoverned space', it is one where the insurgent is determined to fight and win the 'battle for ideas'. 'Twentieth century insurgency' writes Steven Metz, 'sought to eject the state from space it controlled (usually physical territory). Contemporary insurgency is a competition for uncontrolled spaces.'[46] Terrorism and insurgency are distinct, but in many functional respects are closely related forms of ideological and political extremism. As the recently published US Army and Marine Corps Counterinsurgency Field Manual makes clear, much that could be said of cyberterrorism could also be said of cyberinsurgency:

> Interconnectedness and information technology are new aspects of this contemporary wave of insurgencies. Using the Internet, insurgents can now link virtually with allied groups throughout a state, a region, and even the entire world. Insurgents often join loose organizations with common objectives but different motivations and no central controlling body, which makes identifying leaders difficult.[47]

Cyberthreat domain no. 3: serious and organized crime

The Internet has become a hub of personal, political and commercial activity, as well as a vitally important medium for financial and intellectual transactions. It should come as no surprise, therefore, that criminal interest in the Internet has developed accordingly. With the capacity to transmit several hundred billion dollars of economic value via the Internet infrastructure and other IT systems every day, the cyberworld has become a tempting and lucrative target for the modern criminal enterprise. By one estimate there were, for example, some 255,800 cases of online financial fraud in the UK in 2007, with losses amounting to £535 million.[48] Many technologies and software applications are available to enable a wide range of criminal activities in cyberspace to be carried out. But for cybersecurity policy-makers and planners the problem is not just quantitative, but also qualitative and evolutionary.[49] As in other areas of security and defence policy, an action-reaction cycle can be discerned whereby a given cybersecurity measure will prompt a criminal attempt to defeat or bypass it, which in turn will be met by a countermeasure of some sort, and so on. In these circumstances, any description of cybercriminal activities – such as that which follows – can at best be illustrative rather then definitive.

In their biannual *Global Internet Security Threat Report*, the Symantec Corporation describes the variety of tools and systems which are used to criminal ends, the vigour with which they are being deployed, and the main targets of this activity. Basic spam – which may amount to as much as 94 per cent of monitored email traffic[50] – can be used to deliver viruses and Trojans, and as a vehicle for 'phishing' operations, some 80 per cent of which occurred in the financial sector in 2007.[51] Symantec detected over 700,000 new 'malware' (malicious software) threats in 2007. This represented a vast increase in such activity over previous years which they attributed to 'the increasing professionalization of malicious code and the existence of organizations that employ programmers dedicated to the production of these threats'. The goal of all this activity seems clear enough: 'Many of these threats can be used for financial gain by performing actions such as stealing confidential information that can be sold online. These proceeds can then be used to pay the programmers to continue creating new threats.'[52] Black market forums such as ShadowCrew and Darkmarket have used underground economy computer servers for a variety of data-brokering activities; buying and selling stolen bank account details, government-issued identity numbers, credit card details, personal identification numbers and email address lists. In the 'TJX hack' between 2005 and January 2007, for example, a sophisticated criminal operation was able to steal at least 47.5 million credit card numbers.[53] Networks of compromised computers – also known as 'botnets' – are also traded. Symantec detected almost 62,000 bot-infected computers active *every day* from July to December 2007. Botnets can be used to distribute spam and malware, can provide a convincing framework for a phishing campaign, and can be used for large-scale denial of service attacks. The rewards for all this effort can be extraordinary. A single botnet campaign uncovered by the FBI in 2007 caused losses estimated at over US$20m.[54] In 2004, according to the British-North America Committee, the cost to business globally of malware and viruses was between US$169bn and US$204bn, and in 2005 the cost of spam transmissions alone was US$17bn in the US, US$2.5bn in the UK, and US$1.6bn in Canada.[55] It is not inconceivable that an ICT-aware extremist group could use these techniques to overwhelm sections of the Internet in order to reduce significantly the performance of the Internet as a whole, and by so doing marginalize its business benefit.

It is of course important to understand how cybercrime can be carried out, and to what effect, not least in order that appropriate countermeasures can be devised and implemented. But as a 'cyberthreat domain', serious and organized crime is rather more than the sum of the activities described above. The first step towards a closer awareness of the implications of serious and organized crime for cybersecurity is to understand what is meant by the term – and what is not. The meaning of 'crime' is obvious enough: the acquisition of wealth or some other form of benefit through illegal means such as theft, deceit or extortion. 'Organized crime' is less easily defined. The United Nations Convention against Transnational Organized Crime defines an 'organized criminal group' in the following, somewhat vague terms:

> A structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit. […] 'Structured group' shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.[56]

'Serious crime' is a clearer concept. In England and Wales, for example, serious crimes are listed in the Serious Crime Act 2007 and include trafficking in people, drugs and arms; prostitution and child sex; armed robbery; and a wide range of financially-motivated crimes. These last include money-laundering, fraud, 'offences in relation to public revenue', corruption and bribery, counterfeiting, blackmail, and intellectual property offences.[57] As far as the analysis of cybersecurity is concerned, it is significant that the majority of these serious crimes could either be undertaken in cyberspace, or be assisted by some form of cyber-activity. But a simple read-across from real world to virtual world does not provide the most accurate explanation of the emergence of serious, organized crime as a 'cyberthreat domain'. If cybersecurity policy and countermeasures are to be well positioned and effective, then it must be acknowledged that in cyberspace 'serious and organized crime' not only loses some of its coherence as an organizing concept; it can also evolve in response to the unique circumstances of cyberspace.

> 'In 2004 the British Columbia Institute of Technology reported a tenfold increase since 2000 in malicious attacks on process control systems, affecting critical services such as power utilities, sewage systems and wireless networks'

In the first place, it is not the case that all cyberspace crime must be 'organized' before it can be considered 'serious', nor indeed that organized cyberspace crime must necessarily use the most sophisticated means. An illustration of this is offered by low-level computer misuse which can be either an individual (and individualistic) activity, or orchestrated at some level in order to achieve a more dramatic and public effect. The central point to note is that whatever the level of organization at which it takes place, low-level activity and misuse of this sort can be associated with very serious cyber-based criminality. For example, individual hackers (discussed more fully in the following section) can be drawn into the criminal gang culture, using their skills to support drug-related and other crime. When organized in call centres, hackers can systematically set out to implement a large-scale fraud operation, using the simple expedient of having teams of runners available to make illegal ATM cash withdrawals from their victims' bank accounts.[58] For many years businesses with a dominant Internet presence such as eBay, CNN, Yahoo, and Amazon have all experienced denial of service attacks through the receipt of tens of thousands of common junk messages.[59] And in 2004 the British Columbia Institute of Technology reported a tenfold increase since 2000 in malicious attacks on process control systems, affecting critical services such as power utilities, sewage systems and wireless networks. These attacks amounted to 'significant safety, environmental, reputational and financial risks that organizations are running every day.'[60]

When serious and organized crime ventures into cyberspace, it can either continue more or less to conform to traditional definitions and understandings of the type seen in the UK Serious Crime Act, or it can adapt to changed circumstances, evolving into something new and distinctive. In other words, as a 'cyberthreat domain' serious and organized crime can be manifested in two ways: on the one hand, a serious and organized criminal organization can make use of cyberspace in order to continue its criminal activities, while on the other hand a new genre of serious and organized crime can evolve, one that is unique to cyberspace. Choo and Smith draw a distinction between 'traditional organized criminal groups' and 'organized cybercriminal groups'.[61] Cybersecurity policy which overlooks this distinction and which assumes cybercriminality to be a unitary, monolithic threat will almost certainly lack the focus necessary for effective planning.

Serious criminal groups such as the Asian triads, the Japanese Yakuza and East European organizations may exploit cyberspace for a variety of fairly predictable purposes, including money-laundering, drug-trafficking, extortion, credit card and ATM fraud, software piracy, industrial espionage, counterfeit documentation and so on.[62] This phenomenon has usefully been described as 'the migration of real-world organized crime to cyberspace.'[63] For groups of this sort, cyberspace offers new opportunities to acquire vast wealth very quickly. In other words, technology-enabled crime is essentially a new means to a familiar end. Secretive and highly effective organizations such as these, often capable of extreme violence to support or protect their activities, present a serious challenge to national law enforcement agencies, particularly where criminality crosses national borders: 'online crooks can easily jump from one jurisdiction to another, whereas the authorities from different countries have yet to learn how to co-operate'.[64] But all is not lost for law enforcement agencies. Although they may operate in the new world of cyberspace, groups such as the Yakuza retain many of their traditional features, such as a hierarchical structure built upon a culture of loyalty and belonging. Groups such as these are, therefore, to some extent predictable in their organization and their interests, and in what might loosely be described as their 'business practices'.

> ‘Law enforcement will require a decentralized and devolved way of doing things, in order to meet the threat at the moment it develops, and wherever it does so’

The greater challenge to national and international law enforcement could be the organized cybercriminal group, carrying out 'third generation cybercrimes' which are 'wholly mediated by technology'.[65] Groups in this category may have interests very similar to those of their traditionally organized brethren, although cybercriminality might be more conducive to particularly furtive crimes such as paedophilia. But cybercriminal organizations will place far less emphasis on physical strength and the use of force, and will be less concerned to develop an exclusive and extremely loyal membership. As Choo and Smith suggest, the members of a cybercriminal organization might only 'meet' online.[66] The cybercriminal organization will typically be more pragmatic; driven less by gang loyalty than by the need to bring the necessary technological skills together at the right moment: 'In the cyberworld', suggests Brenner, 'physical strength is insignificant [...] strength is in software, not in numbers of individuals.'[67] Indeed, there might be very little need for complex (least of all hierarchical) organization. Brenner argues that an elaborate organizational structure should not be necessary for criminals to operate in a (virtual) world which can be created more or less as the user wishes. Cyberspace is mutable; what the cybercriminal needs, therefore, is agility and responsiveness, rather than structure. If cybercriminality does require some form of organization, it need be no more than a 'Mafia of the moment', which will disappear when no longer needed.[68] Cybercriminal groups will use sophisticated technology and will also have international coverage. The disruption of the Darkmarket forum saw arrests in the United Kingdom, Germany, Turkey and the United States, and followed several years of investigative work. The Deputy Director of the UK Serious Organised Crime Agency described Darkmarket as 'a one-stop shop for the online criminal', before insisting 'these aren't geeks we're talking about. These are serious and organized criminals.'[69]

Cybercriminal groups are likely to adopt flatter, non-hierarchical, more networked and more occasional models of organization, improving their ability to adapt rapidly to changing circumstances, albeit making them more vulnerable to being cut off from any form of leadership that may exist. Nevertheless, variable geometry of this sort could also appeal to extremist groups drawn into criminality for one reason or another. Such groups will value a structure which on the one hand is effective at wealth creation but on the other hand does not require a cumbersome and traceable infrastructure. The law enforcement response to the threat of cybercriminality must be similarly sophisticated and agile, seeking to understand and anticipate the threat as it evolves, appears, disappears and reappears. Law enforcement will require a decentralized and devolved way of doing things, in order to meet the threat at the moment it develops, and wherever it does so. It will also be essential not only that law enforcement agencies be able to cooperate across national boundaries, but also that they remain open to the possibility of a functional relationship between cybercriminality and extremist groups.

Cyberthreat domain no. 4: lower-level/individual crime

At the final point on the notional (and non-hierarchical) spectrum of cyberthreats we find the 'script kiddie', using software tools devised and provided by others to intrude into computer networks, and his more sophisticated and infamous cousin – the hacker. In any analysis of computer hacking a sense of balance is often difficult to maintain; for some analysts hacking should be considered a more or less discrete activity in cybersecurity; but for others it lacks coherence, is not particularly meaningful and is in no sense equivalent to the much more serious cyberthreat domains discussed above. Yet, as we have shown, hacking is often a central feature of these more serious cyberthreats. Hacking is also widely and erroneously seen among the media and in public opinion as the archetypical cyberthreat. For both reasons, therefore, a brief description of hacking is appropriate here.

Stereotypically a troubled and/or bored teenager, with a yawning gap where a normal social life should be, the hacker may actually be highly educated and skilled in programming. But he is motivated, perversely, to compete against himself and his peers, using and testing his skills to intrude into ICT networks, either for his own amusement or to cause gratuitous disruption or damage, for petty theft, or to acquire some celebrity within his peer group. So-called 'digital natives', who have grown up with digital technology and the world of the Internet, are thought to be anxious 'to achieve geekdom immortality', moving beyond mere 'piracy and cheating' in order to 'create a headline-grabbing piece of … malware.'[70] A more sinister version of the individual hacker might be a disappointed customer or a disaffected insider such as a sacked employee who intrudes into his former employer's network to seek revenge by causing damage or who colludes with outsiders as a result of coercion or bribery. More serious still, an individual hacker might see himself acting on an international stage, participating in a grand political or ideological campaign.

The threat from hacking is often overstated and even dramatized, as if the global ICT infrastructure were close to destruction by the incessant efforts of networks of bored youths seeking recreational stimulus. The reality is that for the first six months of 2008, of all security breach incidents reported around the world only 23 per cent could be attributed to the activities of hackers.[71] Nevertheless, it is clear that the consequences of individual hacking can be anything but low-level. On some occasions the motive is far from recreational, and the hacker concerned is revealed to have been acting apparently with clear purpose in mind. Accused of hacking into scores of government computers in 2001 and 2002, Glasgow-born Gary McKinnon admitted to planning attacks in response to what he perceived to be the post-9/11'terrorism' sponsored by the United States. McKinnon's case also shows how government responses to the activity of hackers can vary widely. When the UK National Hi-Tech Crime Unit (NHTCU) tracked down McKinnon in 2002, he was informed that he might face community service, among the most lenient of punishments available to the British courts. That same year, however, although he had not been charged by the UK Crown Prosecution Service, he was nevertheless indicted by the United States government. After an appeal process lasting up to 2008, McKinnon finally lost his case in the UK and the European Union and was set for extradition to the United States.[72]

The grave dangers associated with hacking are also acknowledged and dramatized in the world of fantasy and fiction. In the 1983 thriller War Games a teenage hacker from Seattle initiated a process which could have resulted in nothing less than the outbreak of 'World War III', had he been unable to bring things to a halt. This fictional account appears to have had an inspirational effect; in a case of life reflecting art, since the 1980s there have been numerous media reports of teenagers hacking into supposedly secure military and government systems. This is a trend that seems set to continue.

Summary

The four cyberthreat domains discussed here – state-sponsored cyberattacks; ideological and political extremism; serious and organized crime; and lower-level/individual crime – present a broad range of often interconnected hazards and risks with which security policy-makers must contend. Hacking is a relatively low-level and disorganized activity, yet it can have very high-level consequences, and also features prominently in other threat domains. Serious and organized criminal misuse of the global ICT infrastructure is increasing, in both quantitative and qualitative terms, and at considerable cost to the global economy. The Internet seems to fit the requirements of ideological and political extremists particularly well, and governments can only expect the 'ungoverned space' of the global 'infosphere' to remain closely and bitterly contested. Finally, at the level of states and governments, it would appear that in some quarters the Internet is increasingly viewed in straightforward and all too familiar terms: as a strategic asset to be exploited for the purposes of national security, and perhaps even as a battlefield where strategic conflict can be won or lost. The central observation we draw is not simply that increasing dependence on ICT infrastructure creates vulnerabilities and opportunities to be exploited by the unscrupulous, but also that ICT has an increasingly important enabling function for serious and organized crime, ideological and political extremism, and possibly even state-sponsored aggression.

3 Cybersecurity: Practices and Principles

'Cyberspace' clearly means many different things to many very different constituencies. As we have shown, the global ICT infrastructure provides an efficient and effective networking tool for people and organizations. The unprecedented capacity for real-time communications has fostered a climate of spontaneity and entrepreneurialism in business, nationally and internationally. In political terms, there is a republican quality to the electronic communications revolution; a global technological commons has been established,[73] and the bars to entry are moving ever lower. As the Internet becomes more firmly embedded as a global public good, for some it even offers the prospect of a progressive realignment of global politics along cosmopolitan liberal lines. But like any common good, cyberspace has also proved to be open to misuse. In Chapter 2 we have shown that however many benign uses there might be for the Internet, it is also open to misuse by hackers, criminals and extremists, and is even becoming seen as both a battlefield and a weapon in interstate conflict. Unfortunately, cyberspace seems especially conducive to uses and users of these sorts.

It follows that 'cybersecurity' must also have many different meanings, as various sectors of life and society seek to protect themselves and their interests from a range of potential harms. This is not to argue that 'cybersecurity' has so many meanings for so many people that it has become a meaningless and useless term. The opposite is true: cybersecurity means *too much*, rather than being meaningless, and is used *too often and too seriously* for it to be useless. But when it is understood from many different perspectives, each of them valid and urgently felt, the general effect is one of disjointedness. If cybersecurity can only be understood in terms of this or that narrow context, then it becomes impossible to understand it as a strategic problem and to act accordingly. This is problematic, since in its many permutations cybersecurity represents a challenge to society as a whole, even though society appears unable or unwilling to respond in a similarly holistic manner. In this chapter we argue that a common conception of cybersecurity is necessary in order not only to understand the breadth and depth of the problem, but also as a basis for policy-making in the public and private sectors, and as the context in which individual responses can be informed and made. If governments, businesses and individuals are to make the best use of limited resources and are to ensure that their decisions and actions complement rather than conflict with each other, then a common conception of cybersecurity will be essential.

We begin with a review of current initiatives and procedures in cybersecurity policy. We then outline a range of principles, both strategic and operational, according to which a more coherent cybersecurity policy might be shaped.

Cybersecurity: current practice

Cybersecurity has been conceptualized in several different ways and has prompted a wide range of policy responses. These responses can generally be described as 'bottom-up' insofar as they represent a unit-level response to perceived cybersecurity threats and challenges. The unit concerned may be an individual, but it may also be a commercial entity or a government department. The key point here is that the threat is perceived and analysed in the unit's own terms, reflecting the unit's interests and preferences, and the response is tailored by, and is proportionate to, the unit's capabilities and expertise. We begin our description with the vast numbers of individual ICT users, for whom the problem has been one of ensuring ***computer security and network security***. At this low level, responses and solutions have been disconnected and often largely technical. Next to be considered are organizational efforts (both private-sector and governmental) to ensure ***information security*** and its close relative ***information assurance***. Finally, at the level of government as a whole, there is the approach known as ***Critical National Infrastructure Protection (CNIP)***.

Computer security and network security

For the individual user, cybersecurity is best understood as a combination of computer security and network security. ***Computer security*** is concerned with the protection of the system (both hardware and software) and the information it carries from theft, corruption or interdiction. It can therefore involve both physical measures, such as limiting access to ICT systems and controlling the user base, as well as digital security enhancements, such as the creation of a secure ICT architecture and operating system, and the use of secure coded software and anti-virus software. To an extent, the goal of computer security is to ensure security at the level of the component parts of the system. This approach should as a consequence improve the security of the ICT system as a whole. The computer security approach is largely protective and reactive, in that physical and digital security measures are designed either to limit unauthorized access or to react to a software vulnerability once it has been identified. It follows that in computer security, a good deal of initiative must rest with the illicit actors who can continue to devise political and digital intrusions until they find one which does not elicit a full-scale defensive response. A parallel can be found in the context of terrorism, where it is often said that the attacker need be lucky only once, whereas the defender must be lucky all of the time. In fact, a sophisticated terrorist attack would probably require the perpetrators to be 'lucky' on many occasions and in many different settings if their elaborate plan is to work.[74] What might at least be said is that in computer security it seems to be the defender who has the most difficult time, and whose resources are often of patchy quality. With regular updates required (in some cases daily) by most commercial off-the-shelf anti-virus software, for example, computer security is labour- and cost-intensive and inefficient. Furthermore, any security advantages are at best temporary victories.

Computer security is complemented by ***network security***. When vulnerabilities arise – as they must – from connection to a network, it becomes necessary to safeguard 'computer networks and the information they contain from damage or disruption.'[75] Network security is achieved, once again, through a combination of physical measures to prevent unauthorized access to the network and to network-accessible resources and equipment, and electronic measures to protect the computing network infrastructure. Network security therefore encompasses a wide range of tools, including administrative and physical controls, and on the electronic side firewalls, encryption and authentication software, anti-virus and intrusion-detection systems. These defensive/reactive measures are proving increasingly ineffective, however. According to a recent UK government assessment, UK companies can suffer many security breaches every day, and over 50 per cent of large businesses experience up to hundreds of attempts to break into their networks daily.[76]

Computer security and network security are serious and sophisticated approaches to cybersecurity, based on careful planning and preparation. Both approaches function, essentially, in the area of the so-called 'known knowns' – the source, seriousness and style of likely cyber-attacks, the extent of vulnerability to such attacks, and so on – and can offer effective responses within these parameters. But these responses are closely scripted, configured to meet certain types of challenge from certain quarters. Computer security and network security, with their combination of physical security protocols and technological security measures, will be less robust in the face of novel threats and so-called 'wicked' problems, and might be overwhelmed by a rapidly expanding array of security challenges. If cybersecurity is understood narrowly in terms of the 'bottom-up' approach offered by computer security and network security, then the only conclusion to be drawn is that cybersecurity is by definition obsolescent. There would seem to be two ways to avoid this trap. The US National Institute of Standards and Technology (NIST) has claimed that 'Many of today's tools and mechanisms for protecting against cyber attacks were designed with yesterday's technology in mind.'[77] The first option, therefore, might be to seek a 'bottom-up, high-capacity' approach, whereby the most sophisticated cybersecurity capability is distributed to the lowest levels, including businesses and private individuals.

> ' Bottom-up improvements in technological capacity as well as top-down acceptance of more overall responsibility must be part of an effective and durable cybersecurity regime '

Something like this idea surfaced in an August 2008 report of the Science and Technology Committee of the House of Lords. The committee recorded the public perception of the Internet as 'a lawless "wild west"' and was uneasy that the UK government might have 'distributed' too much responsibility for cybersecurity to the under-equipped individual.[78] This comment could, of course, lead to a very different judgment as to the best way to avoid obsolescence in cybersecurity. Rather than focus on improving the lot of the 'under-equipped individual' through the distribution of more sophisticated technology, the second option could be to reverse the distribution of responsibility, insisting instead that government and central authorities assume more control over, and responsibility for, the cybersecurity system as a whole. As we suggest generally in this report, both options – bottom-up improvements in technological capacity as well as top-down acceptance of more overall responsibility – must be part of an effective and durable cybersecurity regime. Difficult questions then arise: how can responsibility for cybersecurity be distributed between the private (individual), commercial and governmental domains? And as far as public policy is concerned, who within government should take ownership of which aspects of the cybersecurity challenge, charged with developing and articulating policy?

Information security and information assurance

At one level, both the private commercial sector and national governments have adopted a technological approach to cybersecurity, usually summarized by the term ***information security*** (IS). Driven by the need to safeguard e-commerce, the private sector in particular has been concerned to protect information and information systems from unauthorized access and interference. A comprehensive definition of IS has been provided by the US government:

> The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide — (a) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (b) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (c) availability, which means ensuring timely and reliable access to and use of information.[79]

Private-sector/commercial IS has also been addressed by multilateral organizations.[80] The European Union's European Network and Information Security Agency (ENISA) initiative, for example, has focused on IS as a means to facilitate the flow of legitimate e-commerce. In Article 2 of ENISA's charter, the goal of the agency is described as enhancing 'the capability of the Community, the Member States and, as a consequence, the business community to prevent, address and to respond to network and information security problems.'[81]

With its primary concern to ensure the flow of data, IS embodies what might be termed an objective or quantitative approach to cybersecurity. Furthermore, IS concentrates on specific types of attack and, as with computer security and network security, is very largely a reactive posture. Addressing a relatively narrow range of events and effects, the IS model has less interest in underlying causes. Arguably, therefore, IS has less to offer to the analysis and understanding of the global ICT infrastructure as a whole, and to the generation of a coherent, comprehensive and above all anticipatory approach to cybersecurity.[82]

Information assurance (IA) is usually understood to be very closely related to IS. There are considerable overlaps in usage of the two terms, and as a result some argue that they should be merged, or that a new omnibus term should be introduced. Yet, at least for the present, the two expressions do have somewhat different meanings. If IS can be understood as a largely reactive policy of defence and denial, with an emphasis on technological and physical solutions to the security of data and data systems, then IA is more qualitative, in both method and outcome. Giving some sense of this qualitative shift, the UK Cabinet Office defines the goal of IA as 'the confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.'[83] IA takes an approach which is more strategic than IS, in that IA might, for example, address the consequences of and the recovery from an information attack, and might offset (i.e. accept) a data risk in one area by achieving a level of security in some other area. IA should therefore be understood as the ***management of risk*** where the quality, reliability and availability of information are concerned, using the standard tools of mitigating, excluding, accepting or transferring risk, and doing so cost-effectively. As such, IA should be expected to make more of a contribution than the narrower IS approach to the development of cybersecurity strategy.

Organizationally, in the UK information assurance policy is driven by the Wider Information Assurance Centre (WIAC), with policy implementation being undertaken by a variety of governmental bodies including the Central Sponsor for Information Assurance (CSIA) in the Cabinet Office, the Centre for the Protection of National Infrastructure (CPNI – discussed below), the Communications-Electronics Security Group (CESG – the UK national technical authority for information assurance, and a part of GCHQ, the Government Communications Headquarters), the Department for Business, Enterprise and Regulatory Reform (BERR), the Home Office and the e-crime unit of the Serious and Organised Crime Agency (SOCA). With so many agencies and departments involved in IA-related activities, it would seem that the United Kingdom has sought to adopt not only a qualitative but also a broad-spectrum approach to this aspect of cybersecurity.

Critical National Infrastructure Protection

Critical National Infrastructure Protection (CNIP) is the cross-governmental effort to protect vulnerable and interconnected national infrastructures, covering a wide variety of services. In the United Kingdom the interdepartmental Centre for the Protection of National Infrastructure (CPNI) advises government and appropriate non-governmental agencies, as well as those sections of commerce and industry whose services and products form part of the Critical National Infrastructure (CNI). The UK government defines the CNI as those assets, services and systems that support the economic, political and social life of the UK whose importance is such that any entire or partial loss or compromise could cause large-scale loss of life; could have a serious impact on the national economy; could have other 'grave social consequences'; or could be of immediate concern to the national government. The CPNI arose from a merger, on 1 April 2007, of the National Security Advice Centre (NSAC) and the National Infrastructure Security Co-ordination Centre (NISCC), both formerly part of the Security Service. NSAC had been responsible for providing advice on physical and personnel security, while NISCC's task had been to provide advice and information on computer network defence and information assurance. Before the merger, NISCC had joint accountability to the Director of GCHQ and employed staff from GCHQ's Communications Electronics Security Group (CESG). By extending and formalizing this cross-departmental approach, the CPNI incorporates physical, personnel and cybersecurity specialisms into a single, publicly acknowledged body. The CPNI also works closely with the private sector and with international partner organizations. The CPNI thus provides security advice in both the physical and the virtual domains, works within and between governments, acts as a bridge between the public and the private sectors and has brought cybersecurity more into the mainstream of security policy.[84]

Strategic principles of cybersecurity

A general policy for cybersecurity would be one which enables the alignment of the various concerns, interests and approaches operating in the realm of cybersecurity: the individual, the corporate and the national; the technical, the political and the economic; the bottom-up 'tactical' with the top-down 'strategic'; and the public with the private. One way to achieve alignment across and within all sectors might be to make one perspective (national security, for example) the priority and organize all others around it. We argue, however, that the foundation of a more integrated and robust cybersecurity regime requires a common conception of cybersecurity – both the problem and responses to it. At the strategic level, a common approach to cybersecurity can be encouraged by observing the principles of governance, management and inclusiveness.

Governance

The governance of cybersecurity should consider three things. First, cybersecurity should have a normative dimension. That is to say, policy should be configured in such a way that it privileges legitimate users, while increasing the costs for illegitimate users. Second, cybersecurity should have a collective dimension, involving as many legitimate stakeholders and agencies as necessary and feasible. Clearly, where openings remain in critical infrastructure protection or in information assurance, these are likely to be sought out and exploited by criminals and aggressors. The protective fence must, in other words, be unbroken and of uniform height. A collective approach will also mean that cybersecurity becomes a self-reinforcing dynamic environment; if each participant can learn from the experience of others, the sum of cybersecurity should increase. As well as the normative and the collective, there is also a quantitative dimension to the governance of cybersecurity, in that cyberspace (and its myriad uses) remains a vast, complex and constantly evolving phenomenon which cannot be controlled, managed or even overseen by any one user or stakeholder. By this analysis, the governance of cybersecurity amounts to a *self-governing* effort by a *wide range of legitimate users* of cyberspace, and it is difficult to see how such an effort could be made other than in a climate of transparency and accountability. Effective and durable governance of cyberspace requires a shared awareness, which might alternatively be described as a culture of cybersecurity. Drawn up in 2002, the OECD *Guidelines for the Security of Information Systems and Networks* emphasize the need to move away from technological concerns and definitions towards an understanding of the broader environment. The OECD *Guidelines* describe this environment as a culture of security in which 'due account' is taken 'of the interests of all participants, and the nature of the systems, networks and related services' and in which action is guided by nine principles, among them 'awareness', 'responsibility', 'ethics' and 'democracy'.[85]

Management

Cyberspace could be described (albeit not calculated) as the sum of countless interactions among countless users of the global ICT infrastructure. To achieve absolute, perfect security in cyberspace would require all malign users and components to be identified and isolated, and certain interactions to be interdicted. But to do so – even if it were possible – would be to contradict the very essence of cyberspace as a technological global commons; a worldwide 'republic' of communications and information exchange. According to Vinton Cerf, popularly known as the 'father of the Internet', 'if every jurisdiction in the world insisted on some form of filtering for its particular geographic territory, the web would stop functioning.'[86] If perfection is not feasible – and perhaps not even desirable, given the constraining effect it would have on the Internet – then the requirement must be to *manage* rather than *eliminate* threats and risks which come from cyberspace. Furthermore, rather than hope in vain to anticipate every imaginable cybersecurity contingency, a more mature approach would be to devise a cybersecurity regime which has the flexibility and durability to meet contingencies as they develop. Cybersecurity thus becomes a matter of ***risk management***.

Risk can be defined as a compound of threat (or natural hazard), vulnerability and impact. Where cybersecurity is concerned, risk must be understood in the broadest possible sense, and at the level of society as a whole, as 'the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.'[87] Risk management in this context becomes a matter of identifying ICT vulnerabilities and potential threats or harms, followed by an assessment of countermeasures and the assignment of 'differential and often limited resources to sometimes incompatible priorities',[88] in order to reduce either likelihood or impact, or a combination of both. The goal of risk management is to reduce risk to an acceptable level (by mitigating, excluding, transferring or accepting risk) and by doing so to improve the prospects for security. Risk management is necessarily an iterative process; countermeasures must be constantly re-evaluated as new assets emerge, as priorities and vulnerabilities change and as threats evolve. And clearly, where the assignment of scarce resources is involved, a balance must be struck between the cost and the effectiveness of a given countermeasure, and the value of the asset being protected. Furthermore, in a complex network environment the risk/reward evaluation by one actor must be set against the possibly very different risk/reward calculus of other actors.

Inclusiveness

Given its technological sophistication, the rapidity of its evolution and the diversity of its user base, the global information infrastructure could be described as an overwhelmingly complex problem for analysts, industrialists and policy-makers alike. The complexity of cybersecurity can result in a preference for a largely technical language, where awkward and unpredictable political nuance can be kept at bay. This tendency should be avoided where possible. Although cybersecurity is, to a considerable extent, a matter of technology, technology alone is not a sufficient basis for policy; an approach to cybersecurity which is entirely or largely technological might lack the breadth necessary to ensure the broadest possible understanding of, participation in and response to cybersecurity challenges. Yet cybersecurity policy which deliberately marginalizes those with technological expertise – the so-called 'technorati' – makes the equal and opposite error. If the preferred response to complexity is to simplify and to reduce the problem to more manageable components, then the policy process will have excluded those who could have a central and decisive role in the evolution, adaptation and effectiveness of cybersecurity policy.

> 'As cyberspace evolves, so the threats and challenges which emanate from it should also be expected to evolve'

Understanding the intersection between the technical, the social and the political goes to the heart of the problem of solving, or even merely mitigating, the problem of cybersecurity. Cyberspace is better understood as a global information and communication environment, where technology is not only an entry point to the debate, but also a vitally important driver of change. Cyberspace is a diverse arrangement of technology, products, collaborative environments and applications. These elements all interact in a constantly evolving system which is largely dynamic and unpredictable. Furthermore, this system is driven by a vast and diverse array of stakeholders – some more benign than others – including individual users, ad hoc communities, the private sector, the public sector, the national security community and of course the 'technorati'. Self-evidently, technology contributes considerably to the evolution of cyberspace. And as cyberspace evolves, so the threats and challenges which emanate from it should also be expected to evolve. In order to understand and ideally to anticipate these shifts in cyberspace and in the nature of threats and challenges to society, there is a convincing case for involving the 'technorati' yet more closely in the development and implementation of policy, even at the highest levels of national security. They are, after all, those most likely to understand developments in cyberspace, and involving them more closely should lead, in the policy process, to a clearer understanding not only of the ways in which cyberspace is likely to evolve, but also of the threats and challenges that might emanate from it.

Furthermore, if for their part the 'technorati' can develop a clearer sense of the constraints and requirements of national security, it might even be possible to steer the evolution of cyberspace in more benign directions.

Operational principles of cybersecurity

We have argued that the first step towards a common conception of cybersecurity is to agree upon a set of principles – discussed above – by which strategy can be guided. Policy coherence at the strategic level can nevertheless be undermined by inconsistencies in implementation. At the operational or implementation level, various additional principles might be identified, such as agility and initiative, actor neutrality and risk management.

Agility and initiative

The range of cyberthreats is so broad and mutates so quickly that a static, defensive stance (an 'electronic Maginot Line') will mean two things. First, the agile and intelligent cyberadversary will enjoy a good deal of initiative in the struggle, and will not have had to compete particularly vigorously to gain that initiative – a relatively docile and complacent opponent will have surrendered it. Second, the response to cyberthreats will be reactive, rather than anticipatory (or pre-emptive). In other words, the point at which society, the commercial sector and individuals begin to address cyberthreats is the point at which those threats are fully formed and at their most potent. Cybersecurity policy should therefore seek as much agility in implementation as can be achieved, and should focus on winning and maintaining the initiative.

Actor neutrality

In terms both of threat and response, an 'actor neutral' approach to cybersecurity can help to ensure that energy and resources are applied promptly and efficiently and where they can be of most benefit. With a diverse and evolving set of cyberadversaries, it is arguably less important to know the identity and ambitions of the adversary than to know what an adversary (*any* adversary) could do, and to have the policies, procedures and equipment necessary to meet (or anticipate) that challenge, whatever the source and whenever it occurs. This approach is borrowed from the 'capability-based' (as opposed to 'threat-based') approach to military planning: As far as the nature of the response is concerned, at the very least it is essential to move away from definitions of cybersecurity which correspond to the roles and interests of this or that department of government or private-sector concern, towards a common management of the problem. One way to encourage a more standard and inclusive response to cybersecurity challenges would be, once again, to focus less on the identity of the adversary and more on those elements of the risk equation – vulnerability and impact – which society itself can do most to mitigate.

Risk management

It would not be reasonable to expect to eliminate all cyberthreats, permanently: threats are diverse and constantly evolving, and it will be impossible to filter out all criminal or hostile use (actual or potential) of the global ICT infrastructure. This situation is in part caused by widespread dependence on ICT; a global public good has been created, and the barriers to entry are low, if not non-existent. Dependence cannot be eliminated and neither, consequently, can exposure and vulnerability to cyberthreats. If threat, dependency and vulnerability cannot be excluded, they can nevertheless be managed. A risk management approach to cybersecurity would:

- Indicate that legitimate use of ICT cannot be assumed to be free of plausible adverse consequences;
- Enable cybersecurity to be assessed on the basis of proportionality: perceived benefits can be set against possible penalties, and benefits can therefore be prioritized;
- Encourage agility and adaptability: as cybersecurity challenges evolve, priorities can be recalibrated;
- Allow cybersecurity policy to be framed at a system level, with risks and dangers in one sector being offset by benefits and advantages in another.

Summary

As described in Chapter 2, hacking, cybercriminality, terrorism and insurgency, and cyberaggression are all features of what amounts to a system-level challenge to society. This is problematic, essentially because society itself does not act and respond as a coherent system where cybersecurity is concerned. Stakeholders remain segregated and concerned with security within their narrow ambit, and as a result fail to see that they can be affected by another stakeholder's security, or lack of it. Thus the business community can be narrowly focused on cybercrime, even though cybercriminality increasingly exploits techniques and technology which have migrated from the world of espionage, for example. Equally, anti-government hackers have been known to use the techniques of cybercriminals. The first step in meeting this general challenge would be to accept in principle that cybersecurity policy can and should be extended beyond its default settings; the largely reactive and 'bottom-up' or sectoral concerns with computer and network security, information security and assurance, and the protection of critical national infrastructure. The second step should be to base cybersecurity policy on an agreed set of strategic and operational principles, with the following objectives: to turn cyberspace from a permissive, ungoverned environment into a self-governing network; to heighten the costs of use by illicit actors; to encourage a comprehensive and inclusive understanding of cybersecurity across society; and to facilitate and assure legitimate use of the global ICT infrastructure. The breadth of the cybersecurity challenge is such that modern society could be said to be threatened comprehensively or systemically. A system-level response will be necessary to meet a system-level threat, in order that the activities of different agencies and bodies complement each other and are mutually reinforcing, rather than conflicting. Yet an approach to cybersecurity which draws in a very wide range of agencies and organizations, conceivably from all sectors of society including scientific and technical experts, is scarcely one which will be susceptible to central direction. There is a need, therefore, for approaches at the strategic and operational levels which are to a large extent self-informed, self-governing and spontaneous, yet which form part of an overall, mutually agreed framework, or regime.

4 A National Cybersecurity Regime

We have described cybersecurity as a problem in two parts. In the first place, dependence on ICT, on the part of governments, commercial enterprises and individuals, creates vulnerability. And as dependence increases in the global information revolution, so too does vulnerability. The second part of the problem is the dilemma of the technological commons. Criminals, terrorists and other miscreants are all able to exploit the same ICT networks and systems on which legitimate users depend, in order to attack those users in some way. The dilemma is clear: a restrictive approach to the global technological commons might narrow the scope of action of illegitimate users, but it would also constrain the behaviour of legitimate users, for whom a permissive (and perhaps even unregulated) ICT environment would be preferable. In these circumstances, it becomes difficult for legitimate users to move beyond a passive or self-preserving stance, whereby illegitimate users are tolerated as the inevitable corollary of legitimate uses of the commons. As a result, cybersecurity postures have generally, but not exclusively focused on defensive capabilities, intended to protect individual users and lawful businesses against the damage caused by hackers, identity thieves, cyberbrokers and so on.

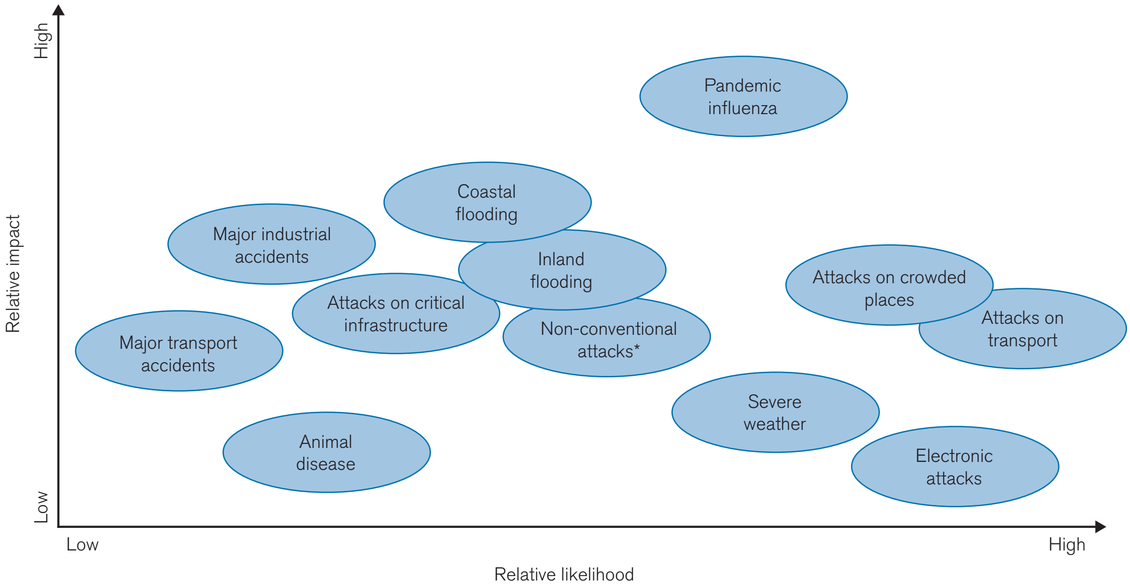
As the information revolution progresses, cybersecurity must be understood as more than a list of threats to be reviewed and amended from time to time, more than a problem of technology or engineering, and above all more than a matter largely of defence and self-preservation. We contend that a new approach to cybersecurity will be required, one which is both more inclusive and more active. The case for an inclusive approach was set out in the previous chapter, with the argument for a common conception of cybersecurity. We show in this chapter how this common conception becomes the basis of a national cybersecurity regime. By this approach, the dual problem of cybersecurity – the relationship between dependency and vulnerability, and the dilemma of the technological commons – can be turned from weakness into strength. We make this argument in three steps, drawing on the experience of the United Kingdom. First, we show how a common, national conception of cybersecurity can be achieved by making use of the United Kingdom's *National Risk Register*. Second, we show how this common conception might then be given substance as an active strategy for cybersecurity. And finally we show how this strategy might be operationalized in the form of business process analysis and interdiction.

The United Kingdom *National Risk Register*

A useful basis for a common understanding of and common approach to cybersecurity is provided by the UK Cabinet Office's *National Risk Register*, published in August 2008.[89] Within its first pages the *National Risk Register* provides a visual representation of relative likelihood and impact of 'high consequence risks facing the United Kingdom'. The authors of the document are cautious, making clear that 'due to the nature of the risks contained within each grouping, it is not possible to represent an exact comparison but only to give an idea of the position of each group of risks relative to others, in terms of likelihood and impact.'[90] Nevertheless, in spite of their caution the result is a straightforward and useful graphic, reproduced in Figure 1.

There are several things to be said of this graphic, both presentational and substantive. First, it illustrates the breadth of security challenges with which society might be confronted and, as such, provides the basis for a common understanding of vulnerability. Second, it offers a societal

Figure 1: UK *National Risk Register*: high-consequence risks



* Excluding CBRN terrorism

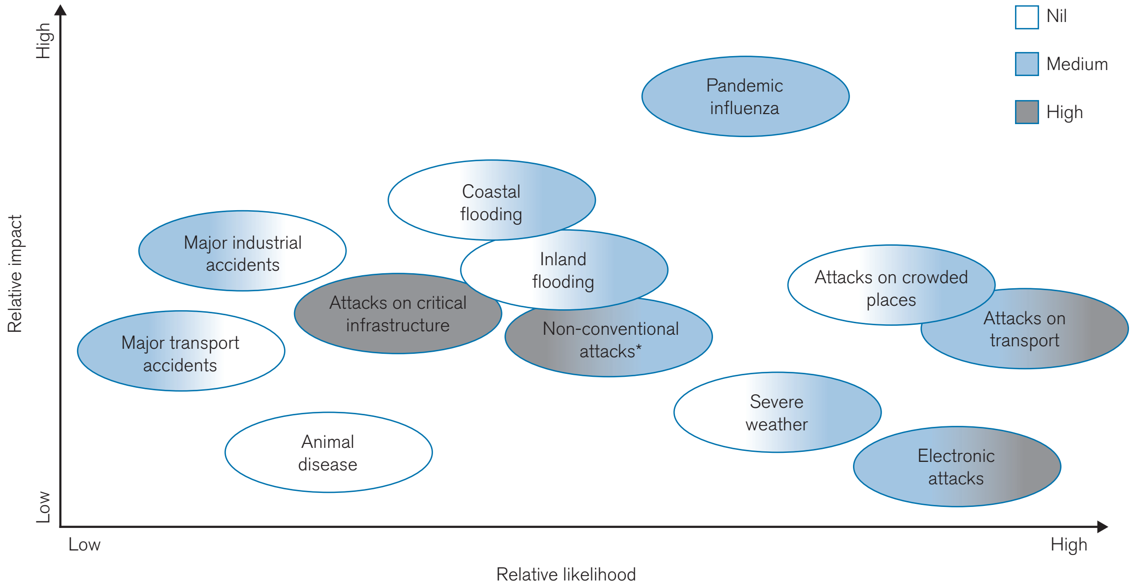
Source: UK Cabinet Office, *National Risk Register* (London: Cabinet Office, 2008), p. 5

rather than a sectoral view of security and is consistent with a cross-governmental or 'comprehensive' approach to national security. It touches on most concerns and functions of modern government, including economic performance, transport and logistics, food supply, security and defence, industry, environment and coastguard, and public health. Given that the *National Risk Register* is produced by the UK Cabinet Office, it could also be described as an approach to security management which is *informed* but not *driven* by central government, and in this respect it is more likely to complement than contradict the 'bottom-up' approaches to security described in Chapter 3. More substantively, this graphic offers a generic and flexible approach to national security analysis and management, rather than a more rigid model focused on a given threat or range of threats. It allows risks to be moved around or deleted, and new risks to be added as they become apparent; what matters is the idea of risk, and that risk can be identified, graded and managed rationally and proportionately. The graphic also has merit as a visually accessible risk management tool. By setting impact against likelihood (the definition of risk) it encourages prioritization not only of threats (man-made) and hazards (natural) but also of responses. Thus, pandemic influenza is not only the most serious risk represented here; it is also self-evidently the risk which requires an urgent and high-level response. The graphic also provides a framework with which to consider whether those 'high consequence risks' which are relatively less likely or which would have relatively less impact could be managed by mitigating, excluding, transferring or accepting the risk. Finally, and most significantly, as a national risk management tool the *National Risk Register* provides not merely a common sense of vulnerability but also a common, multi-stakeholder conception of national security.

How might this common conception be applied to cybersecurity? On the assumption that the relative positioning of the various risks is reviewed from time to time, we consider that the review process could also cover the ***cyberdependency*** of each risk, through the simple expedient of a shading system. Cyberdependency can be interpreted here from two perspectives. First, there is a level of cyberdependency associated with the activities of governments, businesses or individuals in each of the risk areas that requires a level of protection. Second, there is also a level of cyberdependency in the response to that risk. These can both be represented in the following way. In Figure 2 the cyberdependency of stakeholders' activities and functions can be represented by the shading on the left of each risk, while the cyberdependency of their response can be represented on the right. Thus, 'electronic attacks' will expose varying degrees of cyberdependency: in this example a stakeholder's cyberdependency might be medium, shown in blue to the left, while the response might be highly cyberdependent, shown in grey to the right. Pandemic influenza might also expose cyberdependency but at a medium level (coloured blue): some key ICT workers might be incapacitated by the epidemic, and ICT networks might experience greater demand than usual as efforts are made to manage the epidemic effectively. In this example, both sides of the risk would be coloured blue. Finally, animal disease might have little effect on the cyberinfrastructure and might not cause much additional demand on ICT capacity; it could therefore be shown in white for low cyberdependency in both function and response.

Figure 2 could have a number of uses in cybersecurity analysis and response. First, it establishes and locates the idea of cyberdependency within the broad field of national security analysis and policy-making. The model could also assist in the development of a common operating picture for cybersecurity. Government departments and agencies and commercial organizations could be invited to contribute to and improve the model by providing advice as to cyberdependency in those risk packages with which they are most concerned. Third, the model allows cybersecurity effort to be prioritized. The priority for cybersecurity efforts could be those risk packages which show a combination of high impact, high likelihood and high cyberdependency – i.e. 'Attacks on critical infrastructure' and 'Non-conventional attacks'. Next in importance could be those risk packages which are highly cyberdependent and *either* high impact *or* high likelihood – i.e. 'Electronic attacks'. The model then provides a broader framework for cost-benefit analysis in cybersecurity responses. Given limited financial resources, governments, businesses and individuals could address and prioritize those risk packages which show medium cyberdependency. It should be possible to assess the cost of a given cybersecurity effort against expected benefit within each risk package, and then to make an overall assessment across the model as a whole. Thus, if a cybersecurity effort in 'Coastal flooding' would be high-cost but of marginal benefit, it could take second place to 'Attacks on transport' where the opposite

Figure 2: High-consequence risks: illustrating cyberdependency



* Excluding CBRN terrorism

Source: UK Cabinet Office, *National Risk Register* (London: Cabinet Office, 2008), p. 5

calculation might have been made. Finally, the model is versatile: it could be scaled down to meet the requirements of regional or local government, or scaled up to the inter-governmental level, e.g. the EU; and the model is also transferable between public and private sector, for example.

An active strategy for cybersecurity

Cybersecurity, as we have argued throughout this paper, is much more than a traditional problem of national security or of conventional military defence. Nevertheless, if the language of conventional warfare were to be applied to cybersecurity, society could be described as being engaged in a long-term attritional conflict (i.e. trench warfare), but against a weaker adversary which acts differently (i.e. 'asymmetrically'), which is flexible and which moves too fast for the mechanics of a highly structured response to interdict. In conventional military terms, this would not be considered a favourable battlefield encounter. Accordingly, at its simplest what is required is for society to transform its ability to match or, better still, to overtake the speed of the opponent and thereby to seize the initiative. However, a more detailed analysis of the conflict space is required. Since society is resource-limited and cannot afford (and probably would not want) a broad-spectrum approach to cyberspace denial, it must instead focus its most appropriate capabilities against critical elements of illegitimate organizations and structures. And the problem of the global technological commons should always, of course, be borne in mind: any initiative that impinges unnecessarily on legitimate use of cyberspace will be met with significant disapproval and possibly defection.

An active strategy for cybersecurity can be developed in a series of steps: by establishing an ***agile organization*** for cybersecurity; by articulating a national ***cybersecurity doctrine***; by careful ***planning and deconfliction***; and finally through ***responsiveness***.

Agile organization

Chapter 2 describes a wide range of cybersecurity threats and challenges, many of them well known and observable, and covered in detail by the media. These activities are also acknowledged in a corresponding range of security measures and protocols put in place by public and private authorities, and described in Chapter 3. Yet for all the awareness of the cybersecurity problem, and for all the breadth and complexity of the countermeasures, it cannot yet be said that comprehensive, counterbalancing cybersecurity policies are fully operational. Society, broadly understood, is of course becoming progressively more engaged in the cybersecurity problem. But so far that engagement has been largely passive, defensive and uncoordinated; both 'agility' and 'organization' seem in short supply. With the exception of some national (and classified) capabilities related to 'information operations', and associated with military capability, there are few offensive capabilities that can be directed in a timely fashion against the broad range of cyberadversaries. Exceptions to the rule would include self-starting, unregulated groups such as the *Internet Haganah*,[91] along with others such as right-wing Christian organizations which, in the absence of government-led operations, are combating Islamist-related cyber campaigns on their own initiative. In terms both of scope and of substance, however, efforts of this sort can scarcely be said to represent society's best response to the challenge of cybersecurity.

While cybersecurity strategies lack agility and organization, the problem is compounded. A passive stance on the part of society permits faster-thinking, faster-moving and unregulated actors to dominate cyberspace, operating essentially on their own terms. These people, groups and gangs have almost unlimited freedom of manoeuvre. Being unencumbered by any requirement to comply with legislative or operational protocols, they can be opportunistic and dynamic. While society reacts defensively, cyberadversaries, at whatever level they operate, can achieve significant operational advantages in the virtual world because their decision/action cycle (the so-called 'OODA loop': Observe, Orient, Decide, Act[92]) is significantly faster and much less complicated than that of public authorities or commercial bodies, and operates relatively free of interference from these bodies.

The goal of an agile and active organization should be to limit cyberadversaries' use of the technological commons – the global ICT infrastructure – while at the same time ensuring that the commons remain accessible to legitimate users. This goal can be achieved in three ways: first by making illegal activity so dangerous or costly that cyber-adversaries abandon their cause altogether; second by forcing cyberadversaries to abandon cyberspace and to continue their illicit activities in the physical world, where they will be more vulnerable to observation and interdiction by security and law enforcement agencies; and finally by disrupting adversaries' activities within cyberspace in order to lengthen their decision/action cycle, making them more susceptible to intelligence oversight and making it possible for security and law enforcement agencies to decide and act faster than their adversaries. If these goals are to be achieved (and the overall effect required will probably be some combination of the three outcomes), then law-abiding entities (commercial, leisure or academic, for example) should be able to continue to use cyberspace with minimal fear of inadvertent disruption caused by over-regulation of the environment. In other words, one of the principal aims of a cybersecurity strategy should be to reduce both harmful effects to, and unnecessary constraints upon the information environment.

The current UK response to the exploitation of cyberspace by adversaries lacks both agility and organization, making it difficult to achieve these goals systematically and efficiently. Governmentally, the response is more multi-agency than inter-departmental; a characteristically 'stovepiped' posture, with different agencies responding in different ways to different perceptions of cybersecurity. There have recently been attempts at a more coordinated effort, not least the creation in April 2007 of the Centre for the Protection of National Infrastructure (CPNI), described in Chapter 3. Yet while there is certainly enough defensive capability available (in the CPNI itself, in the use of Original Equipment Manufacturer's (OEM) licences for technology, and in self-help precautions for individual ICT users) there is no national-level capability, at least in the law enforcement domain, that is able to take the initiative to the adversary, other than some limited examples in child protection and counter-terrorism intelligence operations. Significantly, Service Oriented Architectures (SOA), in which larger systems are composed of more numerous but less tightly coupled 'Lego bricks' of computing capability, have emerged as a practical instrument to reduce stovepiping among stake-holder groups, although the full potential of this initiative does not yet appear to have been exploited in the cybersecurity domain.

In cybersecurity, organization is a prerequisite for agility; without it, interaction between stakeholders and actors will be inefficient and ineffective. The various agencies and bodies involved (public and private) will find that they do not operate with the same aim and in accordance with the same set of principles. Planning and preparation will be limited in scope, with operations conducted, at best, on an ad hoc basis. One way to counter this problem and to achieve a more organized and disciplined approach would be to establish a *primus inter pares* among the various organizations concerned with cybersecurity; in the UK this would include the Police service, HM Revenue and Customs, the Border Agency, the Serious Organised Crime Agency, the Security Service, the intelligence services and several others. The purpose of such an exercise would be to articulate a unified, cross-governmental plan for cybersecurity to be implemented by all agencies involved. We argue, however, that this approach would not be conducive to agility in cybersecurity; a centrally organized plan for cybersecurity is likely to be too elaborate and bureaucratized, too inflexible and unable to keep pace with events. A better approach would be to organize a national cybersecurity posture around concepts (and perhaps even ethics), rather than around bureaucratic structures and hierarchies. The UK may already have an appropriate policy vehicle, in the form of the Transformational Government initiative. This is intended to formalize ICT interoperability (along the lines of SOA principles) in order to focus better on the users of IT (i.e. those who use IT to support their business processes) rather than upon IT suppliers.[93] An approach of this sort would require that interoperable IT architectures support (rather than drive) a business process-led policy which would in turn encompass doctrine, planning and deconfliction, and responsiveness, to which we now turn.

Cybersecurity doctrine

To a large extent, doctrine is a matter of intellectual discipline and consistency. Thus, a national cybersecurity doctrine would seek to standardize analytical and decision-making methodologies both *horizontally* across the spectrum of governmental activity, and *vertically* from the highest level (i.e. strategic) down to the lowest (i.e. tactical or individual). But the more important question to which doctrine provides the framework of an answer is not '*How* is this to be done?', but '*Why*?' Doctrine would therefore make explicit the fundamental principles by which the various responding agencies' actions would be guided in support of national objectives. If cybersecurity doctrine could be made a national priority, it should have the effect of promoting both joint activity and understanding between governmental 'stovepipes', leveraging best practice currently retained (and in some cases hidden) within separate departments and agencies, and would connect the cybersecurity efforts of governmental agencies and non-governmental bodies (such as commercial firms). It would, of course, be necessary for doctrine to be consistent with the body of UK security policy, particularly the *National Security Strategy*, and to shadow closely any operational plans currently undergoing development or revision (in the UK's case the *National Security Strategy* itself, as well as the Pursue, Prevent and Protect capability strands in CONTEST – the UK counter-terrorism strategy).

Doctrine should be concise and generally comprehensible, setting out broad principles to allow maximum flexibility as the cybersecurity scenario progresses. Consistent with the basic principles of risk management, the core of a national cybersecurity doctrine might be a list of methods and objectives intended to guide cybersecurity policy and operations, such as the following:

- To raise the costs so that adversaries are less inclined to pursue their goals in or through cyberspace;
- To force adversaries and their networks to surface into the physical world where they must function at a slower pace and where they are more vulnerable to identification and interdiction;
- To disrupt the adversary's activity inside cyberspace, lengthening their decision/action cycle and making them more visible to intelligence and investigative processes;
- To cause dislocation of an adversary's business processes by causing internal workflow dysfunction;
- To identify the top-level infrastructure or critical nodes that will enable law enforcement agencies to operate more effectively and disruptively;
- To foster an environment of delegated and distributed authority in order to promote spontaneity, self-confidence and responsibility among responding agencies.

Planning and deconfliction

To achieve agility in cybersecurity, the planning process should have the capacity to focus on rapidly moving targets and should seek to avoid administrative and bureaucratic drag. The most appropriate way to achieve this would be for the planning process to be as decentralized, contextualized and spontaneous as possible, yet without losing overall consistency among the various agencies involved. Consideration should be given to the development of cross-governmental understanding, through the articulation of a common analytical picture (or 'common conception of cybersecurity', as discussed in Chapter 3). Common operational principles should also be agreed, which might additionally include a constant focus on the overall purpose of the cybersecurity activity; the efficient use of scarce resources; flexibility and responsiveness in decision-making; and the use of surprise to dislocate an adversary and force uncharacteristic errors (and perhaps even procedural and psychological paralysis). Having established the broad principles of a common planning approach, adversaries should also be subjected to cyberdependence analysis. This information, made widely available to all relevant agencies, will be the key to effective targeting and will require constant monitoring: the cyberadversary must be presumed to be inherently flexible and likely to change communications protocols very rapidly across cyberspace.

Effective planning is also a matter of deconfliction. Coordination will be required between cyberoperations and more conventional operations, and there should be full understanding of the doctrinal principles and constraints which might obtain in the law enforcement and security sectors, for example. Provision must also be made for the lawful use of cyberspace. Unintended effects and unnecessary constraints on normal commerce could rapidly have a dysfunctional effect on cyberspace, leading to an early breakdown of consensus. Synthetic environment modelling should be able to highlight the hazards to lawful use of cyberspace, and might have the additional benefits of refining law enforcement workflow models and predicting the adversaries' most likely actions.

Responsiveness

To achieve responsiveness in cybersecurity, the decision-making process will require delegated and distributed powers of authority in order to encourage spontaneity and to enable rapid results. The process must also be driven by a statement of the desired outcome and underpinned by a legislative framework with robust but flexible protocols. Results should be gauged by rapid follow-up assessments of whether the desired outcome has been achieved. A closer synthesis of analysis and decision-making – possibly supported by artificial intelligence processing – will also be needed to anticipate the adversary's most likely response once it recognizes that it is under pressure. This will in turn enable pre-emptive activity by law enforcement or security agencies, all with the aim of staying within the adversary's OODA loop. Of the many enablers that would contribute to the generation of responsiveness in cybersecurity, the following are of particular importance:

- A command and control system which can delegate authority to the lowest appropriate level;
- The facility for constant and all-informed coordination of activities among a range of agencies;
- A leadership comprising high-quality, well-trained personnel who are trusted and who have agreed freedoms of manoeuvre;
- Intelligence-led operations at the lowest level practicable;
- Clearly understood limits on actions permitted in the face of observed activity by the adversary;
- Independent and empowered oversight to provide appropriate checks and balances.

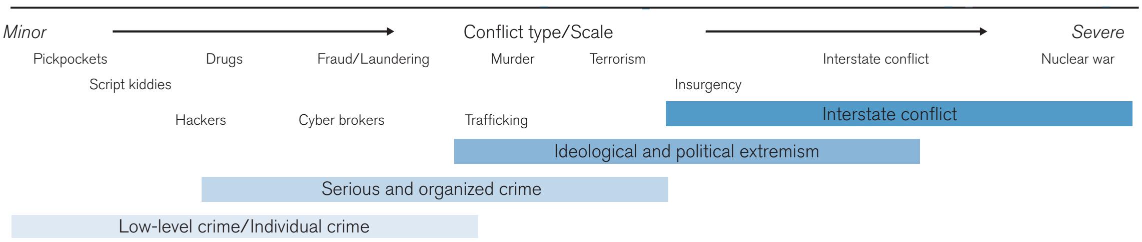
The operational level: business process analysis and interdiction

We have shown how a common conception of cybersecurity can be achieved and how the notion of cyberdependency can validate and reinforce this common conception. This common conception can then be given substance in the form of the active strategy for cybersecurity discussed above. The final step in our argument for a national cybersecurity regime is to show how cyberdependency is much more than a metaphor for society's vulnerability and weakness and can be transformed into a positive advantage in the struggle against cyberadversaries: adversaries are cyberdependent too, and are also vulnerable. There are currently, however, insufficient tools with which to model the end-to-end susceptibility of the cyberdomain to support illicit or adversarial activity. Our first step, therefore, is to suggest a conflict spectrum which in turn will become the basis upon which to analyse adversaries' cyberdependency.

Conflict spectrum

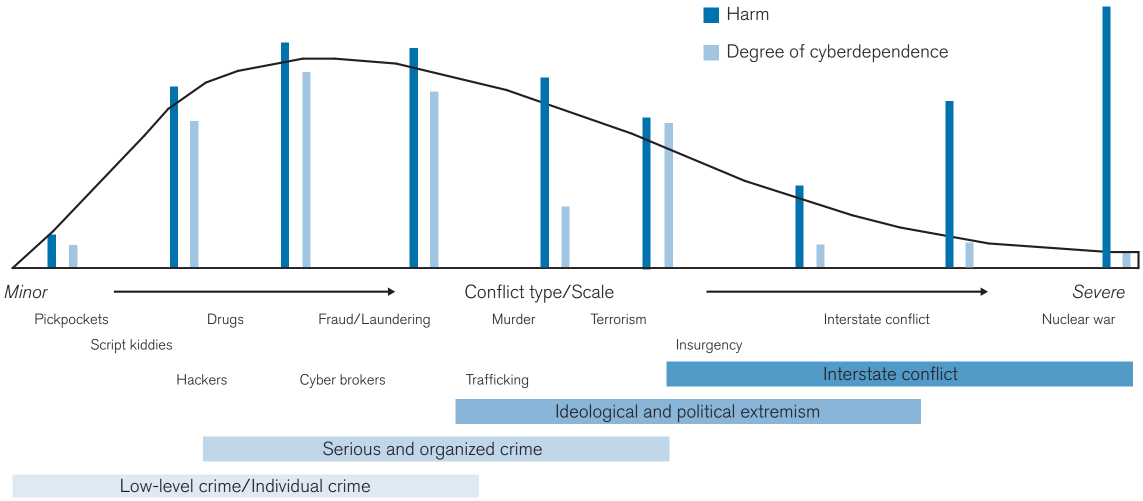
A spectrum could be drawn which maps potential conflicts from very low-order crime, such as pickpocketing, through murder and terrorism, to global insurgency, to interstate armed conflict, and culminating in nothing less than a nuclear exchange along the lines feared during the Cold War. A spectrum of types and levels of conflict,

Figure 3: Conflict spectrum



Source: Morgan Aquila 2009

Figure 4: Conflict spectrum illustrating cyberdependency



Source: Morgan Aquila 2009

incorporating the four cyberthreat domains discussed in Chapter 2, is shown in Figure 3.

Cyberdependency analysis

Elements of this conflict spectrum can be analysed further not only to identify the harm likely to be caused to society at each point of the spectrum (and therefore to judge the severity of the threat), but also to assess the extent to which each threat is dependent upon cyberspace *as part of its business process*. Cyberdependency analysis can be incorporated in the conflict spectrum, as shown in Figure 4.

Business process analysis

A business process-led methodology now introduces some new dynamics. Standard business and risk modelling can identify critical weaknesses in the adversary's ability to continue operations, with the key focus being on identifying bottlenecks (which are abhorrent to business) and other processes which are vulnerable to disruption and which may have no, or poor, backup modes.

Risk assessment matrix

The next step in the process is to construct a risk assessment matrix of the adversary's organization as a preliminary to targeted activity against the critical nodes identified. Persistent disruptive attacks in cyberspace will inevitably lead to business change by the adversary actor, and ideally a return to the physical domain where the adversary's decision/action loop will lengthen, because real-world constraints (the requirement to travel or use surface mail) will inevitably cause a reduction in the pace of their activity. In the first place, this approach will require careful consideration and mapping of the adversary's internal processes (as illustrated in the value chain model in Figure 5). It then becomes possible to identify bottlenecks and cybercritical nodes, and to assess how and where to interdict the key processes, as Figure 5 shows.

A more sophisticated and selective approach to value chain interdiction is illustrated in Figure 6.

The business process/value chain interdiction model is a tool for to identifing and exploiting the adversary's own cyberdependency and vulnerability; what we have identified as a structural weakness on the part of society is thus transformed into a useful tool. Furthermore, it is a tool that is easily comprehensible and widely applicable. Yet for all its merits, the business process methodology can be challenged in a number of respects. The phenomenon of the 'information blizzard', for example, might well cloud the picture and could require a shift in the data/intelligence management dynamic, possibly towards

Figure 5: Value chain model – interdiction

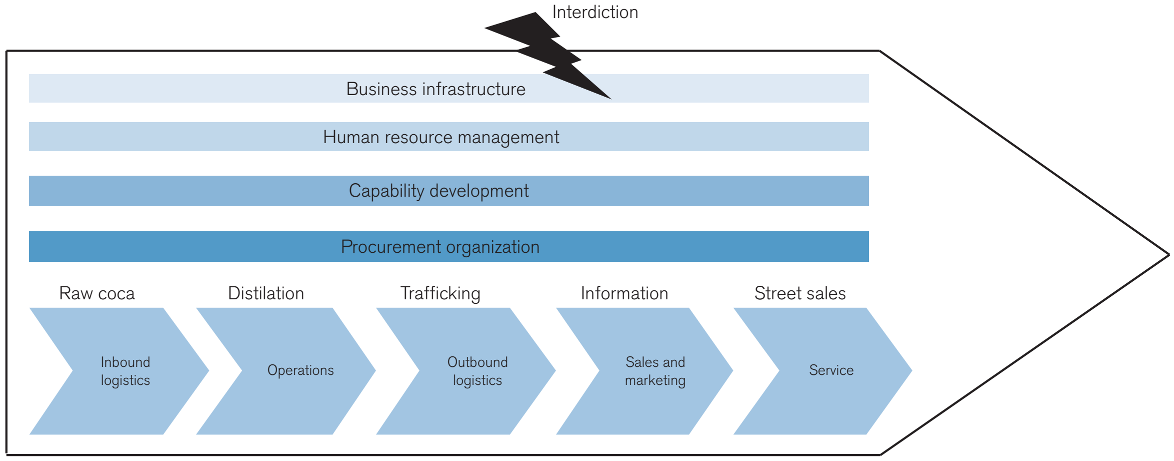
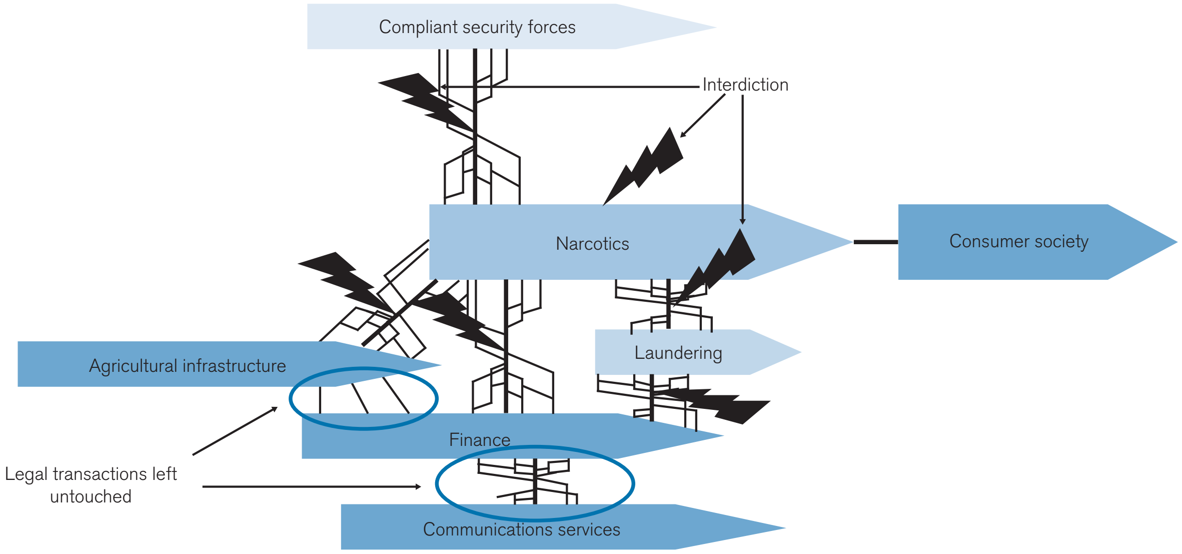


Figure 6: Selective value chain interdiction


Compliant security forces
Interdiction
Narcotics
Consumer society
Laundering
Agricultural infrastructure
Finance
Legal transactions left untouched
Communications services

a 'feed the monster' data-intensive approach. Furthermore, where critical node analysis is concerned, future success might be described as a matter not so much of finding the proverbial 'needle in a haystack', but of finding, in among the mass, a particular piece of straw of the right length, width and colour. A challenge of this sort would require a new look at data extraction and information analytics. And in order to support the 'human in the loop', there would be a need for real-time or near real-time surfacing and visualization of threat activity, in order to enable more rapid changes in the orchestration of the response than the adversary can cope with. In other words, to enable a human-led response there must be a step change in technology to support the decision-making process, to create agility and flexibility on the part of the law enforcement and security response.

Summary

One frequently used definition of a regime in international politics is a set of 'implicit or explicit principles, norms, rules and decision-making procedures around which actors' expectations converge in a given area of international relations. Principles are beliefs of fact, causation and rectitude. Norms are standards of behaviour defined in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action, decision-making procedures are prevailing practices for making and implementing collective choice.'[94] In other words, according to this definition, regimes offer a way to inform and organize effort in public policy, while remaining loosely federal rather than centrally driven or overly directive. A successful and durable regime is one which functions intelligently and responsively within its area of concern, and which is sufficiently elastic to maintain a unified approach as circumstances change.

We argue that the regime offers the most suitable basis for a national cybersecurity strategy which must include (yet not direct) a wide variety of actors, agencies and stakeholders, and which must be sufficiently agile (yet without losing focus) to meet a rapidly evolving and transforming security challenge. Our first step was to show how the recently published UK *National Risk Register* could help to achieve greater coherence among the various agencies involved in cybersecurity; a 'top-down' approach which could complement the 'bottom-up' security measures set out in Chapter 3. Furthermore, an adapted version of the *National Risk Register* could be used to explain and develop the idea of cyberdependency. Our next step, moving from theory to practice, was to show how an active strategy for cybersecurity could be achieved, by giving consideration to agile organization, doctrine, planning and deconfliction, and responsiveness. Finally, we showed how cyberdependency could be much more than a structural weakness on the part of society and could become an operational tool in a national cybersecurity strategy, using the example of business process analysis and interdiction.

5 Conclusion

Any analysis of cyberspace and the security threats it entails should first acknowledge that this is not the concern exclusively of governments and public authorities, commercial enterprises, or individuals. Cybersecurity is a problem which concerns everyone, particularly as society becomes ever more dependent on the global ICT infrastructure, and therefore vulnerable to interference by adversaries able to act within or against ICT systems. In cyberspace, different interests and constituencies are challenged by a variety of interconnected actors and actions. And if society – for all its diversity – cannot respond in a similarly interconnected way, then the sum of security diminishes overall.

The challenge of cybersecurity can be described in terms of a spectrum of cyberthreat domains: state-sponsored cyberattacks; ideological and political extremism; serious and organized crime; and lower-level/individual crime. The value of this spectrum is more presentational than analytical, however. Lower-level and individual crime such as computer hacking can appear trivial and to lack organization, but it can have high-level consequences and can feature prominently elsewhere on the spectrum. Serious and organized criminal misuse of the global ICT infrastructure is increasing, in both quantitative and qualitative terms, and at considerable cost to the global economy. The Internet seems to fit the requirements of ideological and political extremists particularly well, and governments can expect access to and use of the global technological commons to remain closely contested. Finally, for some states and governments it is clear that the Internet is seen as a strategic asset to be used for the purposes of national security, and perhaps more simply still as a battlefield where strategic conflict can be won or lost. The key observation here is not simply that society's increasing dependence on ICT infrastructure creates vulnerabilities and opportunities to be exploited by adversaries, but also that ICT has an increasingly important enabling function for serious and organized crime, ideological and political extremism, and state-sponsored aggression. In other words, society's adversaries are also ever more dependent upon ICT systems, creating a counterbalancing set of vulnerabilities.

> 'The various illicit uses of cyberspace amount to a system-level challenge to society'

The various illicit uses of cyberspace amount to a system-level challenge to society. This is problematic because society does not act and respond as a coherent system where cybersecurity is concerned. Stakeholders remain largely segregated, concerned to maintain security within their narrow ambit. As a result public bodies, commercial enterprises and private individuals can all fail to see that they are affected by another stakeholder's security, or lack of it. Cybersecurity policy can and should be extended beyond its default settings – the largely reactive and 'bottom-up' or sectoral concerns with computer and network security, information security and assurance, and the protection of critical national infrastructure. It should then be possible to shape cybersecurity policy in accordance with the general principles set out in Chapter 3: governance, management and inclusiveness. Acting coherently and purposively, the various agencies and bodies involved should have as their goals to turn cyberspace from a permissive, ungoverned environment into a self-governing network; to increase the costs of use by illicit actors; to encourage a comprehensive and inclusive understanding of cybersecurity across society; and to facilitate and assure legitimate use of the global ICT infrastructure.

As cybersecurity policies and processes are transformed in these ways, it becomes reasonable and useful to describe these efforts as aspects of a national cybersecurity regime.

Regime thinking offers a way to inform and organize effort in public policy, while remaining loosely federal rather than centrally driven or overly directive. A regime should be responsive to change and should be sufficiently elastic to maintain a coherent approach as circumstances evolve. A national cybersecurity regime would involve a wide variety of actors, agencies and stakeholders, yet would not require a tightly disciplined central hierarchy and bureaucracy. It would also have the agility to meet a rapidly evolving and transforming security challenge, yet without losing purpose and focus. Drawing upon recent experience in the United Kingdom, Chapter 4 described in outline how such a regime might be achieved. The recently published UK *National Risk Register* (to be revised in 2009) provides the basis for greater coherence and a common understanding among the various agencies involved in cybersecurity; a 'top-down' approach which could complement the 'bottom-up' security measures set out in Chapter 3 above. For the purposes of this report, an adapted version of the *National Risk Register* can be used to explain and socialize the central idea of cyberdependency. The next step, moving from theory to practice, is to show how a regime-based approach can generate a national strategy for cybersecurity, by giving consideration to agility and organization, cybersecurity doctrine, planning and deconfliction, and responsiveness. Finally, in order to mitigate both the likelihood and the impact of illegal and extremist activities, a national cybersecurity regime can make use of business process analysis in order to identify the adversaries' cyberdependencies and vulnerabilities. Their weaknesses can then be exploited and their efforts degraded, thereby reducing cyber-enabled risk to society as a whole.

Society faces considerable risk from and within cyberspace, and it must respond appropriately. Whether it does so in the form of a national cybersecurity regime or by some other means, the response must be as effective, as efficient and above all as agile as possible. Yet dealing with the problem of cybersecurity is as much a matter of the quality and comprehensiveness of the response as it is one of identifying and countering cyberthreats. In important respects, the quality of the response will be determined by process and procedure, by effective coordination and by timely decision-making. But cybersecurity also poses complex structural challenges which society must address in all sectors and at all levels. How (and on what authority) should responsibility for cybersecurity be distributed between the private (individual), commercial and governmental domains? As far as public policy is concerned, which government department should be charged with developing and articulating policy, and which departments should take ownership of the various aspects of the cybersecurity challenge? Addressing such questions effectively requires a close and mutually supportive engagement by a triumvirate of key actors: policy-makers at various levels of government, technical experts – the so-called 'technorati' – and not least all lawful users of the global ICT infrastructure. Society must have the knowledge, the agility and the resilience to meet and preferably to anticipate the constantly evolving challenge of cybersecurity.

Notes

1. 'Let it rise: A special report on corporate IT', *The Economist*, 25 October 2008, p. 3.
2. S. Fafinski and N. Minassian, *UK Cybercrime Report 2008* (Garlik, September 2008), pp.12, 21: http://www.garlik.com/static_pdfs/cybercrime_report_2008.pdf.
3. 'Let it rise', p. 7.
4. A. Sipress, 'An Indonesian's Prison Memoir Takes Holy War into Cyberspace', *Washington Post*, http://www.washingtonpost.com/ac2/wp-dyn/A62095-2004Dec13?language=printer, 14 December 2004.
5. 'Cyberjamming', *Wall Street Journal Europe*, 29 April 2008.
6. M. Reilly, 'When nations go to cyberwar', *New Scientist*, 23 February 2008.
7. I. Thomson, 'Nato builds cyber-security bunker', *Information World Review*, 15 May 2008.
8. T. Skinner, 'War and PC', *Jane's Defence Weekly*, 24 September 2008.
9. Reilly, 'When nations go to cyberwar'.
10. M. Fickes, 'Cyber Terror', *Government Security*, 1 July 2008: http://www.govtsecurity.com/federal_homeland_security/cyber_terror_attacks/index.html.
11. Skinner, 'War and PC'.
12. B. Acohido, 'Some Russian PCs used to cyberattack Georgia' *USA Today*, 18 August 2008: www.damballa.com/downloads/news/ITN_USA_Today_2.pdf+Acohido+Georgian+cyber+attack&hl=en&ct=clnk&cd=1&gl=us&client=firefox-a.
13. For an analysis of the scope of cyberwarfare see European Security and Defence Assembly, *Cyber Warfare* (Assembly of the Western European Union, Defence Committee Report C/2022. 5 November 2008).
14. Scott Borg, Director of the US Cyber Consequences Unit, quoted in Fickes, 'Cyber Terror'.
15. US-China Economic and Security Review Commission, 2008 Report to Congress, cited in 'China winning cyber war, Congress warned', *The Guardian* (online), 20 November 2008: http://www.guardian.co.uk/technology/2008/nov/20/china-us-military-hacking.
16. Skinner, 'War and PC'.
17. Ibid.
18. General James Cartwright, Vice Chairman of the US Joint Chiefs of Staff, quoted in Skinner, 'War and PC'. See also Reilly, 'When nations go to cyberwar'.
19. 'World wide web of terror', *The Economist*, 14 July 2007.
20. A. Stenersen, 'The Internet: A Virtual Training Camp?', *Terrorism and Political Violence* (Vol. 20, 2008), p. 228.
21. G. Corera, 'The world's most wanted cyber-jihadist', *BBC News*, http://news.bbc.co.uk/go/pr/fr/-/2/hi/americas/7191248.stm, 16 January 2008.
22. 'World wide web of terror', *The Economist*, 14 July 2007.
23. Corera, 'The world's most wanted cyber-jihadist'.
24. Ibid.
25. D.W. Barno, 'Challenges in Fighting a Global Insurgency', *Parameters* (Summer 2006), p.19.
26. Stenersen, 'The Internet', p. 215.
27. 'World wide web of terror', *The Economist*, 14 July 2007.
28. Distinct from cryptography (the encryption of communications), steganography ('hidden writing') is a means of covert communication in which the message itself (and not just its meaning) is concealed. For added security a concealed message can also be encrypted. See 'Link between child porn and Muslim terrorists discovered in police raids', *The Times*, 17 October 2008.
29. Stenersen, 'The Internet', p. 219.
30. J. Emigh, 'Terror on the Internet', *Government Security*: http://govtsecurity.com/federal_homeland_security/terror_internet/, l October 2004.
31. Stenersen, 'The Internet', p. 233, note 53. MMORPGs and Massively Multiplayer Online Games (MMOGs) can also be used for financial crimes such as extortion and money-laundering, since MMOG and MMORPG players must exchange real currency for virtual cash (such as Linden Dollars) in order to participate. See K.R. Choo and R.G. Smith, 'Criminal Exploitation of Online Systems by Organised Crime Groups', *Asian Criminology* (Vol. 3, No. 1, June 2008), p. 49.
32. 'World wide web of terror', *The Economist*, 14 July 2007.
33. US Senate Committee on Homeland Security and Governmental Affairs, *Violent Islamist Extremism, the Internet, and the Homegrown Terrorist Threat*, 8 May 2008 (http://hsgac.senate.gov/public/_files/IslamistReport.pdf), pp. 1, 8.
34. D. Kimmage, *The Al-Qaeda Media Nexus: The Virtual Network Behind the Global Message* (Washington, DC: RFE/RL Special Report, 2008), pp. 17, 21.
35. Stenersen, 'The Internet', pp. 216, 231.
36. Quoted in 'World wide web of terror'.
37. 'Saudis claim Internet responsible for 80 per cent of jihadi recruitment', *Terrorism Focus* (4/13), 8 May 2007.
38. K. Sengupta, 'Spies take war on terror into cyberspace', *The Independent*, 3 October 2008.
39. 'Jihadis publish online recruitment manual', *Terrorism Focus* (5/34), 24 September 2008.
40. S. Drennan and A. Black, 'Jihad online: The changing role of the Internet', *Jane's Intelligence Review*, August 2007.
41. Stenersen, 'The Internet', p. 222.
42. Drennan and Black, 'Jihad online'.
43. 'World wide web of terror', *The Economist*, 14 July 2007.
44. US Senate, *Violent Islamist Extremism*, p. 5.
45. C. H. Kahl, 'COIN of the Realm: Is There a Future for Counterinsurgency?', *Foreign Affairs* (86/6, November/December 2007), p. 175.
46. S. Metz, *Rethinking Insurgency* (Carlisle: US Army War College Strategic Studies Institute, June 2007), pp. 11, 13–14.
47. US Army and Marine Corps, *Counterinsurgency Field Manual* (Chicago: University of Chicago Press, 2007), para. 1-22, p. 8.
48. Fafinski and Minassian, *UK Cybercrime Report 2008*, p. 14.
49. For an assessment of the role of innovation in and against cybercrime, see H. Rush, C. Smith, E. Kraemer-Mbula and P. Tang, *Organised Crime and Illegal Innovation* (London: NESTA, forthcoming 2009).
50. British-North America Committee, *Cyber Attack: A Risk Management Primer for CEOs and Directors* (BNAC, 2007), p. 3.
51. Symantec Corporation, *Global Internet Security Threat Report: Trends for July-December 2007* (Vol. XIII, April 2008: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf), pp. 8, 64, 75.
52. Symantec, *Global Internet Security*, pp. 45-46.
53. CBR Online, 'TJX hack is biggest ever', 30 March 2007: http://www.cbronline.com/news/tjx_hack_is_biggest_ever.
54. Symantec, *Global Internet Security*, pp. 17, 20–22.
55. British-North America Committee, *Cyber Attack*, p. 2.
56. United Nations Convention against Transnational Organized Crime, Article 2 (a) and (c), United Nations General Assembly, A/Res/55/25, 8 January 2001: http://www.unodc.org/pdf/crime/a_res_55/res5525e.pdf.
57. Serious Crime Act 2007, Schedule 1: Serious Offences, Part 1: Serious Offences in England and Wales, Office of Public Sector Information: http://www.opsi.gov.uk/ACTS/acts2007/ukpga_20070027_en_9.
58. B. Acohido, *Zero Day Threat:The Shocking Truth of How Banks and Credit Bureaus Help Cyber Crooks Steal Your Money and Identity* (New York: Union Square Press, 2008), pp. 22–24.
59. 'Cyber-attacks batter Web heavyweights' *CNN.com*: http://archives.cnn.com/2000/TECH/computing/02/09/cyber.attacks.01/index.html, 9 February 2000.

60. 'New and original study on industrial cyber security reveals tenfold increase in number of successful attacks on process control and SCADA systems since 2000', British Columbia Institute of Technology: http://www.bcit.ca/news/releases/newsrelease100404883.shtml, 4 October 2004.
61. Choo and Smith, 'Criminal Exploitation', pp. 39–40.
62. Ibid., p. 40.
63. S. W. Brenner, 'Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships', *North Carolina Journal of Law & Technology* (Vol. 4, Issue 1, Fall 2002), p. 24.
64. 'Clouds and judgment', *The Economist*, 25 October 2008.
65. Fafinski and Minassian, *UK Cybercrime Report 2008*, p. 8.
66. Choo and Smith, 'Criminal Exploitation', p. 40.
67. Brenner, 'Organized Cybercrime?', p. 27.
68. Ibid., pp. 37, 46.
69. 'Fraudsters' website shut in swoop', *BBC News* (online), 17 October 2008: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/uk/7675191.stm.
70. Acohido, *Zero Day*, p. 18.
71. Microsoft, *Security Intelligence Report* (Key Findings Summary: January through June 2008), http://www.microsoft.com/security/portal/sir.aspx.
72. K. Poulsen, 'UK hacker Gary McKinnon plays the Asperger's card' *Wired,* 28 August 2008; 'British UFO hacker Gary McKinnon is coming to America' *Wired,* 30 July 2008: http://blog.wired.com/27bstroke6/2008/08/uk-hacker-gary.html. A judicial review of McKinnon's case is scheduled for June 2009.
73. 'Commons', used in this report in the context of a 'global commons' or a 'global technological commons', is defined in the *Oxford English Dictionary* as 'provisions for a community or company in common', In the sense employed in this report use of the commons is non-rivalled and non-excludable – a public good, in other words.
74. M. Levi argues that terrorists need to be serially 'lucky', which should actually make interdiction *less* difficult than is often assumed: *On Nuclear Terrorism* (Harvard University Press, 2007), p. 7.
75. J. Lewis, 'Cybersecurity and Critical Infrastructure Protection', Center for Strategic and International Studies (Washington, DC), January 2006: http://www.csis.org/media/csis/pubs/0601_cscip_preliminary.pdf.
76. UK Cabinet Office, *A National Information Assurance Strategy* (London: Central Sponsor for Information Assurance, June 2007), p. 6.
77. National Institute of Standards and Technology, 'Comprehensive National Cyber Security Initiative: Leap-Ahead Security Technologies', http://www.nist.gov/public_affairs/factsheet/cyber2009.html, 1 February 2008.
78. House of Lords, Science and Technology Committee, *Personal Internet Security: Follow-Up* (London: The Stationery Office, July 2008. Fourth Report of Session 2007-2008), p. 5; Minutes of Evidence, p. 2, col. 1.
79. US Code Title 44, Chapter 35, Subchapter III (44 U.S.C. Sec. 3542 (2002), 3542(b)(1)), US Code Collection, Cornell University Law School: http://www.law.cornell.edu/uscode/html/uscode44/usc_sec_44_00003542——000-.html.
80. For a review of multilateral efforts at cybersecurity, focusing on the European Union, see P. Cornish, *Cyber Security and Political, Social and Religiously Motivated Cyber Attacks* (Brussels: European Parliament, 2009).
81. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance). http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32004R0460&model=guicheti.
82. Advocates of ISO 27002, the *Code of Practice for Information Security*, might take issue with these observations. With its emphasis on the 'plan, do, check, act' cycle, ISO 27002 arguably seeks to encourage a more anticipatory management of threats.
83. UK Cabinet Office, *A National Information Assurance Strategy*, p. 12.
84. P. Cornish, *Domestic Security, Civil Contingencies and Resilience in the United Kingdom: A Guide to Policy* (London: Chatham House, June 2007), pp. 7–8.
85. Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security* (Paris: OECD, 25 July, 2002), pp. 10–11: http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.
86. Quoted in 'Geography and the Net: Putting it in its Place', *The Economist*, 9 August 2001.
87. UK Cabinet Office, *A National Information Assurance Strategy*, p. 12.
88. E. Gibbs van Brunschot and Leslie W. Kennedy, *Risk, Balance and Security* (London: Sage, 2008), p. 10.
89. UK Cabinet Office, *National Risk Register* (London: Cabinet Office, 2008): http://www.cabinetoffice.gov.uk/reports/national_risk_register.aspx.
90. UK Cabinet Office, *National Risk Register*, p. 4.
91. See http://www.internet-haganah.com/haganah/index.html.
92. Coined by Colonel John Boyd, US strategic analyst and commentator. In combat (indeed, in any walk of life), the goal should be to complete the OODA cycle before the adversary, thereby retaining the initiative and ensuring success. For a full account and explanation of Boyd's insight see B. Berkowitz, *The New Face of War: How War Will be Fought in the 21st Century* (New York: Free Press, 2003), pp. 38–45.
93. See Cabinet Office, Chief Information Officer Council, 'Transformational Government': http://www.cio.gov.uk/transformational_government/index.asp.
94. S. Krasner, 'Overviews', in S. Krasner (ed.), *International Regimes* (London: Cornell University Press, 1983), p. 2.

The International Security Programme

The International Security Programme at Chatham House has a long-established reputation for independent and timely analysis, and for its contribution to the public debate on security and defence. International security policy is a vast, complex and urgent environment for research and analysis. With this in mind, the mission of the programme is to be an internationally recognized and respected policy research group, offering independent, expert advice for the public and private sectors on matters of international, European and national security and defence.

Recent publications include:

US-UK Nuclear Cooperation: An Assessment and Future Prospects
Edited by Jenifer Mackby and Paul Cornish
Co-published with the Center for Strategic and International Studies, August 2008

Coalition Warfare in Afghanistan: Burden-sharing or Disunity?
Timo Noetzel and Sibylle Scheipers
Briefing Paper, October 2007

Global Non-Proliferation and Counter-Terrorism: The Impact of UNSCR 1540
Edited by Olivia Bosch and Peter van Ham
Co-published with Brookings Institution Press and Clingendael Institute, March 2007

The CBRN System: Assessing the Threat of Terrorist Use of Chemical, Biological, Radiological and Nuclear Weapons in the UK
Paul Cornish
Chatham House Report, February 2007

The UK Contribution to the G8 Global Partnership Against the Spread of Weapons of Mass Destruction, 2002–06
Paul Cornish
Chatham House Report, January 2007

EU and NATO: Co-operation or Competition?
Paul Cornish
Chatham House Report, October 2006

Divided West: European Security and the Transatlantic Relationship
Tuomas Forsberg and Graeme P. Herd
Chatham House Paper, co-published with Blackwell Publishing, June 2006

For a full list of publications, please visit http://www.chathamhouse.org.uk/research/security/

Chatham House Reports

Transit Troubles: Pipelines as a Source of Conflict
Paul Stevens | March 2009 | 978 1 86203 210 1

The Outlook for Tokyo: New Opportunities or Long-Term Decline for Japan's Financial Sector?
Vanessa Rossi | March 2009 | ISBN 978 1 86203 213 2

Ready to Lead? Rethinking America's Role in a Changed World
Robin Niblett | February 2009 | ISBN 978 1 86203 209 5

Food Futures: Rethinking UK Strategy
Susan Ambler-Edwards et al. | February 2009 | ISBN 978 1 86203 211 8

The Feeding of the Nine Billion: Global Food Security for the 21st Century
Alex Evans | January 2009 | ISBN 978 1 86203 212 5

Against the Gathering Storm: Securing Sudan's Comprehensive Peace Agreement
Edward Thomas | January 2009 | ISBN 978 1 86203 213 2

Iran: Breaking the Nuclear Deadlock
Edited by Richard Dalton | December 2008 | ISBN 978 1 86203 208 8

A British Agenda for Europe: Designing Our Own Future
Commission on Europe after Fifty | September 2008 | ISBN 978 1 86203 207 1

The Coming Oil Supply Crunch
Paul Stevens | August 2008 | ISBN 978 1 86203 206 4

Ending Dependence: Hard Choices for Oil-Exporting States
John V. Mitchell and Paul Stevens | July 2008 | ISBN 978 1 86203 205 7

The Gulf as a Global Financial Centre: Growing Opportunities and International Influence
Vanessa Rossi | June 2008 | ISBN 978 1 86203 204 0

Lost Opportunities in the Horn of Africa: How Conflicts Connect and Peace Agreements Unravel
Sally Healy | June 2008 | ISBN 978 1 86203 203 3

The European External Action Service: Roadmap for Success
Brian Crowe | May 2008 | ISBN 978 1 86203 202 6

Changing Climates: Interdependencies on Energy and Climate Security for China and Europe
Bernice Lee et al. | November 2007 | ISBN 978 1 86203 196 8

For further information on any of these titles please visit www.chathamhouse.org.uk/publications or call +44 (0)20 7957 5700.

Detica

CHATHAM HOUSE

Chatham House, 10 St James's Square, London SW1Y 4LE
T: +44 (0)20 7957 5700 E: contact@chathamhouse.org.uk
F: +44 (0)20 7957 5710 www.chathamhouse.org.uk

Charity Registration Number: 208223