EUROPEAN PARLIAMENT

DIRECTORATE GENERAL EXTERNAL POLICIES OF THE UNION

STUDY

Policy Department External Policies

CYBER SECURITY AND POLITICALLY, SOCIALLY AND RELIGIOUSLY MOTIVATED CYBER ATTACKS

FOREIGN AFFAIRS

February 2009

EN

EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES OF THE UNION
DIRECTORATE B
- POLICY DEPARTMENT -

STUDY

CYBER SECURITY AND POLITICALLY, SOCIALLY AND RELIGIOUSLY MOTIVATED CYBER ATTACKS

EP/EXPO/B/AFET/FWC/2006-10/Lot4/15
PE 406.997

February 2009
EN

This study was requested by the European Parliament's Committee on Foreign Affairs.

It is published in the following language: English

Author: **Dr Paul Cornish**
Chatham House, **London**

Study carried out within the framework agreement between **ISIS Europe** and the European Parliament

Responsible Official: **Dr Gerrard Quille**
Directorate-General for External Policies of the Union
Policy Department
WIB 06 M 81
rue Wiertz
B-1047 Brussels
E-mail: gerrard.quille@europarl.europa.eu

Publisher European Parliament

Manuscript completed on 2 February 2009.

The study is available on the Internet at
http://www.europarl.europa.eu/activities/committees/studies.do?language=EN

If you are unable to download the information you require, please request a paper copy by e-mail : xp-poldep@europarl.europa.eu

Brussels: European Parliament, 2009.

CYBER SECURITY AND POLITICALLY, SOCIALLY AND RELIGIOUSLY MOTIVATED CYBER ATTACKS

Dr Paul Cornish
Chatham House

EXECUTIVE SUMMARY

This paper examines **Cyber-Security and Politically, Socially and Religiously Motivated Cyber-Attacks**, focusing on the European Union as an international organisation with a fragmented yet developing interest in cyber-security. The paper is presented in three parts. **Part 1** assesses the source and nature of **cyber threats**. Society's increasing dependence on Information and Communications Technology (ICT) infrastructure creates vulnerabilities and corresponding opportunities to be exploited by the unscrupulous, ranging from low-level, individual computer hacking to serious and organised crime, ideological and political extremism, and state-sponsored cyber attacks such as those perpetrated against Estonia in 2007. ICT also has an important enabling function in each of these cases. 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 ICT infrastructure to be ever more closely contested. At the level of states and governments, it is clear that in some quarters the Internet is becoming viewed as a battlefield where conflict can be won or lost. The threats can inter-connect when circumstances demand – terrorist groups, for example, can be sophisticated users of the Internet but can also make use of low-level criminal methods such as hacking in order to raise funds. The challenge to cyber-security policy-makers is therefore not only broad, but complex and evolutionary.

Part 2 reviews current **multilateral initiatives** to address cyber-security, focusing on the work of the United Nations, the Organisation for Economic Co-operation and Development, the Organisation for Security and Co-operation in Europe, the Council of Europe, the North Atlantic Treaty Organisation, and the Group of Eight. In each case, the organisation in question has recognised the breadth and complexity of the cyber-security challenge and that its response to the cyber-security challenge can be but one part of the whole. Although national governments are the most important actors in cyber-security, others have a contribution to make, including industry and the private commercial sector. Within each organisation there are various balances to be struck: between defensive/passive/protective measures, and a more activist or offensive stance; between security measures (of whatever sort) and civil liberties; and finally between securing the specific interests of a given organisation or government, and the more general requirement to create, for the benefit of all legitimate users, an international communications and technological environment which is as hostile as possible to the activities and ambitions of cyber-terrorists and extremists, cyber-criminals and hackers.

Part 3 examines **European Union's** responses to the cyber-security challenge. The EU is very closely engaged in cyber-security but cannot be said to have a comprehensive approach to the problem: the EU's responses are diverse, lack coherence and could at times conflict. The picture emerges of a vast and ambitious undertaking in government and administration, touching upon most conceivable aspects of societal, commercial and private life, yet which appears unable to organise a comprehensive approach to cyber-security challenges which, if taken together, could be said to threaten the EU comprehensively. A more coherent approach could be achieved in one of two ways:

either by uniting the EU's cyber-security efforts around one central strategy (and perhaps even within a new institutional framework); or by seeking a more efficient co-ordination of effort, while maintaining institutional and role specialisations. The latter approach is preferable; a co-ordinated approach reflects more closely the politics and structures of the EU and would be more responsive to the complex and evolving challenge of cyber-security. This approach – described as *Comprehensiveness in Diversity* – would require a more prominent role for the Common Foreign and Security Policy, the establishment within the Council Secretariat of a Cyber-Security Co-ordinator, and the preparation of an EU-wide Common Operating Vision for cyber-security..

CONTENTS

CYBER SECURITY AND POLITICALLY, SOCIALLY AND RELIGIOUSLY MOTIVATED CYBER ATTACKS

Dr Paul Cornish
Chatham House

It is impossible that old prejudices and hostilities should longer exist, while such an instrument has been created for the exchange of thought between all the nations of the earth.
Comment on the transatlantic telegraph cable, 1858.[1]

Our entire history is connected to space and place, geometry and geography. …the region of combat is most definitely physical.… a new generation is emerging from the digital landscape … Digital technology can be a natural force drawing people into greater world harmony.
Nicholas Negroponte, 1996.[2]

I think the Chinese government has been behind many, many attacks – penetrations. "Attacks" sounds like they're destroying something. They're penetrations; they're unauthorized penetrations. And what they're trying to do is espionage. They're engaged in massive espionage, not only in the U.S. government, in the U.S. private sector as well, but also around the world.
Richard Clarke, 2008[3]

INTRODUCTION

The first two quotations above typify the optimism which has often been associated with the electronic information and communications revolution of the past 150 years or so. There is a sense that communication itself will have a palliative effect on international politics, by reducing prejudice and hostility. Furthermore, it might even be that conflict itself will be consigned to history; a feature of the old 'geographical' world which is to be overtaken by Negroponte's new 'digital' version. The third quotation is more pessimistic. Richard Clarke was the principal advisor on counter-terrorism in the US National Security Council under both the Clinton and the George W. Bush Administrations. Elsewhere in this interview, he argues that 'all of our information is being stolen' and that vast sums expended on research and development in key disciplines of engineering, pharmaceuticals and genetics and so on, are effectively being diverted to the benefit of enemies, criminals and the generally unscrupulous.

While espionage and data theft are serious enough, cyber-security (security within, and from cyber-space) is a much broader problem for individuals, businesses, public and private organisations, governments and international organisations. And it is a problem from which there is no easy escape. The information and communications technology (ICT) infrastructure which is being exploited by a wide variety of miscreants is essentially indistinguishable from that used for entirely innocent and legitimate purposes. And these legitimate uses are often not 'optional extras', which society can set aside for reasons of safety and security. In 2009 it is difficult to imagine a major business or organisation that does not rely on advanced ICT, and it is no exaggeration to say that the 21st century economy, and much of society itself, is dependent upon a broadband-enabled, cyber-knowledge complex. With dependence comes vulnerability, and with the cyber-knowledge complex comes an ever widening array of opportunities for the unscrupulous to exploit.

[1] 'What the Internet cannot do', *Economist*, 19 August 2000.
[2] N. Negroponte, *Being Digital* (New York: Vintage Books, 1996), pp. 238, 230.
[3] R. Clarke, 'Seven Questions: Richard Clarke on the Next Cyber Pearl Harbor', http://www.foreignpolicy.com, 14 April 2008.

This paper examines **Cyber-Security and Politically, Socially and Religiously Motivated Cyber-Attacks**, focusing on the European Union as an international organisation with developing interest in cyber-security. The paper is presented in three parts:

- Part 1: an examination of the source and nature of **cyber-threats**;
- Part 2: a review of other **multilateral initiatives** to address cyber-security;
- Part 3: an examination of the **European Union** and its responses to the cyber-security challenge, and a discussion of the role of the **Common Foreign and Security Policy**.

The paper concludes with recommendations regarding the European Union's response to cyber-security challenges.

PART 1: CYBER THREATS[4]

The first step in any analysis of cyber-security must be to chart the range of cyber-threats, by which is meant either security challenges made *via* ICT equipment and networks, or challenges made *to* those equipment and networks. This can be a difficult undertaking, not least because these two broad categories of security challenge can overlap. Microsoft, for example, have 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 just described.[5] The transformation of the Internet from an elite research network to a mass communications medium has altered the global cyber-threat 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 organised along a spectrum running from individual action (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 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 organised crime; organised criminality can be linked to international terrorism; and terrorism can be used a tool of state aggression. This point is made most strikingly in the prison autobiography of Imam Samudra, executed in November 2008 for his role in the 2002 terrorist bomb attack in Bali. In a section entitled 'Hacking, Why Not?' Samudra 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.[6] With that caveat in mind, this paper discusses cyber-threats on four levels: hacking; serious and organised crime; ideological and political extremism; and state-sponsored cyber-aggression.

Threat Level 1: Hacking

In the spectrum of cyber-threats, the starting point is the 'script kiddie', using software tools devised and provided by others to intrude into computer networks, along with 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 facet of cyber-security; but for others it

[4] Part 1 of this paper is drawn from P. Cornish, R. Hughes and D. Livingstone, *Cyber-space and the national security of the United Kingdom* (London: Chatham House, forthcoming 2009).
[5] 'Let it rise: A special report on corporate IT', *The Economist*, 25th October 2008, p.7.
[6] 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.

lacks coherence and is in no sense equivalent to other, more serious threats. The threat from hacking is often overstated and even dramatised; as if 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 of these could be attributed to the activities of hackers.[7]

Yet the consequences of individual hacking can be anything but low-level, and hacking can often be a central feature of the more serious cyber-security challenges discussed below. The hacker might actually be highly educated and skilled in programming. But he is motivated, perversely, to use 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. A more sinister version of the individual hacker might be the disaffected insider, such as a sacked employee who intrudes into his former employer's network to seek revenge by causing damage. More serious still, an individual hacker might see himself acting on an international stage, participating in a grand political or ideological campaign.

Threat Level 2: Serious and Organised 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. The cyber-world 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.[8] Many technologies and software applications are available with which to carry out a wide range of criminal activities in cyber-space.

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 might amount to as much as 94 per cent of monitored email traffic[9] – can be used to deliver viruses and Trojans, and as a vehicle for phishing operations.[10] Symantec detected over 700,000 new malware threats in 2007, representing a vast increase in such activity over previous years which they attributed to 'the increasing professionalization of malicious code and the existence of organisations 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.'[11] Black market forums such as ShadowCrew and Darkmarket have used underground economy

[7] Microsoft, *Security Intelligence Report* (Key Findings Summary: January through June 2008), http://www.microsoft.com/security/portal/sir.aspx
[8] S. Fafinski and N. Minassian, *UK Cybercrime Report 2008* (Garlik, September 2008), p.14: http://www.garlik.com/static_pdfs/cybercrime_report_2008.pdf
[9] British-North America Committee, *Cyber Attack: A Risk Management Primer for CEOs and Directors* (BNAC, 2007), p.3.
[10] 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.
[11] Symantec, *Global Internet Security*, pp. 45-46.

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. Networks of compromised computers – botnets – are also traded. Symantec detected almost 62,000 bot-infected computers active *every day* from July-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 botnet campaign uncovered by the FBI in 2007 alone caused losses estimated at over US$20m.[12] 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.[13]

When serious and organised crime ventures into cyber-space, it can either continue more or less to conform to traditional definitions and understandings of criminality, or it can adapt to changed circumstances, evolving into something new and distinctive. In other words, as a cyber-threat serious and organised crime can be manifested in two ways: on the one hand, a serious and organised criminal organisation can make use of cyber-space in order to continue its criminal activities, while on the other hand a new genre of serious and organised crime can evolve, one which is unique to cyber-space. Choo and Smith draw a distinction between 'traditional organised criminal groups' and 'organised cybercriminal groups'.[14] Cyber-security policy which overlooks this distinction and which assumes cyber-criminality 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 Eastern European organisations might exploit cyber-space 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.[15] This phenomenon has usefully been described as 'the migration of real-world organized crime to cyberspace.'[16] For groups of this sort, cyber-space offers new opportunities to acquire vast wealth very quickly; technology-enabled crime is essentially a new means to a familiar end. Secretive and highly effective organisations such as these, often capable of extreme violence to support or protect their activities, present a major 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.'[17] But all is not lost for law enforcement agencies. Although they might operate in the new world of cyber-space, groups such as the Yakuza retain many of their traditional features, such as a hierarchical organisation built upon a culture of loyalty and belonging. Groups such as these are, therefore, to some extent predictable in their

[12] Symantec, *Global Internet Security*, pp. 17, 20-22.
[13] British-North America Committee, *Cyber Attack*, p.2.
[14] K. R. Choo and R. G. Smith, 'Criminal Exploitation of Online Systems by Organised Crime Groups', *Asian Criminology* (Vol. 3, No. 1, June 2008), pp.39-40.
[15] Choo and Smith, 'Criminal Exploitation', p.40.
[16] 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.
[17] 'Clouds and judgment', *The Economist*, 25th October 2008.

organisation and their interests, and in what might loosely be described as their 'business practices'.

The greater challenge to national and international law enforcement could be the organised cyber-criminal group, carrying out 'third generation cybercrimes' which are 'wholly mediated by technology'.[18] Groups in this category might have interests very similar to those of their traditionally organised brethren, although cyber-criminality might be more conducive to particularly furtive crimes such as paedophilia and certain pornography. But cyber-criminal organisations 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 cyber-criminal organisation might only 'meet' online.[19] The cyber-criminal organisation 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.'[20] Indeed, there might be very little need for complex (least of all hierarchical) organisation in cyber-space. Brenner argues that an elaborate organisational structure should not be necessary for criminals to operate in a (virtual) world which can be constructed more or less as the user wishes. Cyber-space is mutable; what the cyber-criminal therefore needs is agility and responsiveness, rather than structure. If cyber-criminality does require some form of organisation, it need be no more than a 'Mafia of the moment', which will disappear when no longer needed.[21] Cyber-criminal 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.

Cyber-criminal groups are likely to adopt flatter, non-hierarchical, more networked and more occasional models of organisation, improving their ability to adapt rapidly to changing circumstances. Variable geometry of this sort could also appeal to extremist groups drawn into criminality for one reason or another. Extremist groups will value a structure which is on the one hand effective at wealth creation but which on the other hand does not require a cumbersome and traceable infrastructure. The law enforcement response to the threat of cyber-criminality must be similarly sophisticated and agile, seeking to understand and anticipate the threat as it evolves, appears and disappears. Law enforcement will require a decentralised 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 are able to co-operate across national boundaries, but also that they remain open to the possibility of a functional relationship between cyber-criminality and extremist groups.

Threat Level 3: Ideological and Political Extremism

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.'[22] So-called 'cyber-

[18] Fafinski and Minassian, *UK Cybercrime Report 2008*,p.8.
[19] Choo and Smith, 'Criminal Exploitation', p.40.
[20] Brenner, 'Organized Cybercrime?', p.27.
[21] Brenner, 'Organized Cybercrime?', pp. 37, 46.
[22] A. Stenersen, 'The Internet: A Virtual Training Camp?', *Terrorism and Political Violence* (Vol. 20, 2008), p.228.

terrorism' begins with hacking and low-level criminality. Younis Tsouli, described as 'one of the most notorious cyber-jihadists in the world',[23] 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.[24] By these means, Tsouli was to become 'the administrator of one of the most important extremist websites which facilitated contacts between thousands of individuals.'[25] 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 revelation as to the way extremists had become proficient at conducting operational-level planning on the Internet.[26]

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 organisation 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 might 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. The Internet is an anarchic common ground which extremists can exploit in ostensibly unremarkable ways, just as society does, for such purposes as communication and information sharing.[27] The Internet is also especially suitable for use by organisations which are deliberately opaque in their structure and intention. Indeed, as organisations become more opaque and complex, so the value of the Internet increases accordingly, making it progressively more difficult to identify the organisations in question and to track their progress.

In functional terms, the Internet offers a number of useful services for extremists. In the first place, the Internet 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 organised. 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.

---

[23] 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.
[24] 'World wide web of terror', *The Economist*, 14 July 2007.
[25] Corera, 'The world's most wanted cyber-jihadist'.
[26] Corera, 'The world's most wanted cyber-jihadist'.
[27] Stenersen, 'The Internet', p.215.
[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.

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 latterly video recordings. The Internet makes this material vastly more accessible and reproducible, through passive web postings and interactive chat rooms. The Internet can also immortalise a propaganda message; ensuring that the words of an imprisoned or deceased radical leader remain as a source of inspiration. Finally, the Internet 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 recent 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 decentralised organisation (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 jihadist use of electronic media as a function of weakness rather than strength, and argues that they are determined to impose more control and organisation 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 organisations. While it is certainly the case that virtual training and teaching does take place, this does not necessarily form part of a

---

[29] Stenersen, 'The Internet', p.219.
[30] J. Emigh, 'Terror on the Internet', *Government Security*: http://govtsecurity.com/federal_homeland_security/terror_internet/, 1 October 2004.
[31] Stenerseon, 'The Internet', p.233, note 53. MMORPGs and Massively Multiply 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 Choo and Smith, 'Criminal Exploitation', 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), pp. 1,8: http://hsgac.senate.gov/public/_files/IslamistReport.pdf
[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.

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 sympathisers', and more of a 'pre-school of jihad' than a university.[35]

There is generally more agreement on the importance of the Internet for the indoctrination, recruitment and radicalisation of extremists, not least among government agencies. The Dutch domestic intelligence service, for example, describes the Internet as the 'turbocharger' of radicalisation,[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 cyber-extremism 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] But with so many resources available on the Internet, recruitment and radicalisation is no longer simply a matter of 'organisational pull', but is also increasingly a matter of 'individual push' or self-recruitment and self-radicalisation.[40]

Self-radicalisation is an important and intriguing prospect. 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 'homegrown terrorist' can develop; a combination of anonymity and violent potential which is a cause of concern for western intelligence and counter-terrorist agencies. Self-radicalisation also suggests that for extremists the Internet is both much more and, curiously, much less than a global communications network. The Internet offers the means by which not only to proliferate but also to 'atomise' the extremist campaign;[42] the global jihad can be achieved, in other words, without the continued requirement for elaborate communications networks and a well-organised global command structure. Widely dispersed and self-radicalised jihadi 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-radicalised individuals who are then connected with each other, less through the infrastructure of command, control and communications than through a simple common cause.

Once radicalised and trained via the Internet, 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 the Internet has become a 'battle space' in its own right; a

---

[35] Stenersen, 'The Internet', pp.216, 231.
[36] Quoted in 'World wide web of terror', *The Economist*, 14 July 2007.
[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.

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 DOS 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 the terrorist and insurgent to magnify the symbolic effect of his 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]

Threat Level 4: State-Sponsored Cyber-Aggression

The inter-state dimension to the misuse of the cyber-world 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 cyber-operation. Yet the source of the attack was alleged to be none other than 'Europe's longest-ruling dictator, Belarus's Aleksander Lukashenko', reportedly concerned to limit media coverage of opposition protests against his regime.[47]

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 cyber-attacks, 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 cyber-weapons.[48] More recently, the cyber-attacks launched against Estonia in April and May 2007 have captured attention. In a dispute over a Russian war memorial, Estonian government and banking websites and Internet providers were the targets of concentrated DDOS attacks. These attacks were especially disabling for a country which held itself up as a pioneer of electronic government. There was some uncertainty as to who or what had orchestrated the attacks, although the Estonian authorities eventually prosecuted a lone hacker. One important lesson of the Estonian affair was that even very large organisations and government departments are vulnerable to disabling attacks of this sort, and the episode

[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] 'Cyberjamming', *Wall Street Journal Europe*, 29 April 2008.
[48] M. Reilly, 'When nations go to cyberwar', *New Scientist*, 23 February 2008.

hastened NATO's development the Co-operative Cyber Defence Centre of Excellence which had been established in Estonia.[49]

Drawing lessons from the long military tradition of electronic warfare, cyber-operations 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 cyber-attack against Syrian air defences, enabling non-stealthy Israeli aircraft to move into Syrian airspace without fear of detection and interdiction.[50] 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.'[51] This warning rang true within one year, with the Russo-Georgian conflict over South Ossetia in summer 2008. Described as 'the coming of age of a new dimension of warfare',[52] the conflict saw private computing power organised and co-ordinated in such a way as to have strategic effect on a national enemy. It is not clear that the Russian government was directly behind the DDOS attacks on Georgia, but it seems likely that the attacks were officially not prevented, even if not formally approved. Although no serious long-term Georgian cyber damage was reported, the coordinated attack showed an 'untapped potential for using the Internet to cause mass confusion for political gain'.[53]

It is likely, if not certain that cyber-warfare will be an increasingly important feature of conflict between states in years to come. Indeed, losses and gains made in cyber-space 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.'[54] China's intentions and capabilities often feature prominently in analysis of this sort. According to a US Congress policy review panel 'China is aggressively developing its power to wage cyber warfare and is now is 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.'[55] 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 counter-measures, CND would be a crucial feature of cyber-dependent operations, and is consistent with the view that the Chinese People's Liberation Army would seek to

---

[49] T. Skinner, 'War and PC', *Jane's Defence Weekly*, 24 September 2008.
[50] Reilly, 'When nations go to cyberwar'.
[51] M. Fickes, 'Cyber Terror', *Government Security*: http://www.govtsecurity.com/federal_homeland_security/cyber_terror_attacks/index.html, 1 July 2008.
[52] Skinner, 'War and PC'.
[53] 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
[54] Scott Borg, Director of the US Cyber Consequences Unit, quoted in Fickes, 'Cyber Terror'.
[55] US Congress, US-China Economic and Security Review, 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.

achieve 'electromagnetic dominance' early in a conflict, and to maintain that advantage.[56]

If cyber-security does become increasingly militarised, and if the Internet does become one more weapon in a 'state sponsored act of war,'[57] then a number of intriguing political, technological and ethical questions are raised. What is the best form of defence in cyber-warfare? What exactly are 'cyber-weapons'? Are they weapons of war, such as combat aircraft and artillery guns? Is the Internet merely harmless technology, or is to be regarded (like traditional weapons) as something which can be used to damage, destroy and kill, and regulated as such? Is it reasonable or useful to regard cyber-weapons as equivalent in magnitude to 'weapons of mass destruction'?[58] And finally, how could the origin of a cyber-attack, and the identity of the perpetrator, be ascertained?

Summary: Part 1

The four cyber-threat levels discussed here – Hacking; Serious and Organised Crime; Ideological and Political Extremism; and State-Sponsored Cyber-Attacks – present a broad range of often inter-connected hazards and risks with which security policy-makers must contend. Hacking is a relatively low level and disorganised activity, yet it is one which can have very high level consequences, and which also features prominently in other threat levels. Serious and organised criminal misuse of the global ICT infrastructure is increasing, in both quantitative and qualitative terms, and with considerable cost to the global economy. Perversely, 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 is clear that in some quarters the Internet is viewed in straightforward and all-too familiar terms; as a strategic asset to be exploited 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 to 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 organised crime, ideological and political extremism, and state-sponsored aggression.

PART 2: MULTILATERAL INITIATIVES

Part 2 of the paper reviews the work of leading international organisations active in the field of cyber-security. The organisations covered are: the United Nations (UN); the Organisation for Economic Co-operation and Development (OECD); the Organisation for Security and Co-operation in Europe (OSCE); the Council of Europe; the North Atlantic Treaty Organisation (NATO); and the Group of Eight (G8)). In each case, rather than provide an exhaustive analysis of every activity and initiative, the principal characteristics of the organisation's approach to cyber-security are described.

United Nations

[56] Skinner, 'War and PC'.
[57] Skinner, 'War and PC'.
[58] 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'. The WMD analogy is also used in Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection, 17 December 2003: http://www.whitehouse.gov/news/releases/2003/12/print/20031217-5.html.

Cyber-security has been a feature of traditional security policy debates within the UN system, usually associated with the threat of terrorism and in the form of **UN Security Council** Resolutions.[59] The subject is covered in the work of the Security Council's **Counter-Terrorism Committee**,[60] and is mentioned in the UN **Global Counter-Terrorism Strategy**. In the latter case, the aim is not only to 'counter terrorism in all its forms and manifestations on the Internet', but also, in a more activist approach, to 'use the Internet as a tool for countering the spread of terrorism'.[61] More broadly, cyber-security is regularly acknowledged within the UN system to be a central feature of the constantly evolving international security agenda. In December 2002, for example, a **UN General Assembly** debate noted 'the growing dependence' on information technologies of a wide variety of users including governments, commercial organisations and private individuals. As participation in, and dependence upon the global information society increases, so too does the need for cyber-security; the correlate of dependence is vulnerability. But the General Assembly cautioned against assuming that a law enforcement approach to cyber-security would be sufficient; cyber-security 'must be addressed through prevention and supported throughout society.' Similarly, the General Assembly noted that technology could not provide a complete answer to the challenge of cyber-security and spoke of the need for a 'culture of cybersecurity in the application and use of information technologies.'[62] The notion of a 'global culture of cyber-security' was also taken up some years later by Kofi Anna, then Secretary General of the United Nations. In a speech delivered on the occasion of the first World Information Society Day in May 2006, Annan neatly encapsulated the problem of cyber-security:

> In an increasingly interconnected and networked world, it has become critically important to safeguard our vital systems and infrastructures against attack by cybercriminals, while instilling confidence in online transactions in order to promote trade, commerce, banking, telemedicine, e-government and a host of other e-applications. As this depends on the security practices of each and every networked country, business and citizen, we need to develop a global culture of cybersecurity.[63]

This 'soft' or 'cultural' understanding of, and approach to cyber-security is complemented by the more practical approach of the **International Telecommunication Union** (ITU). Within the UN system the ITU has most responsibility for the practical aspects and applications of international cyber-security.

---

[59] See UN Security Council Resolution 1373: reference to 'use of communications technologies by terrorist groups' (28 September 2001, para. 3(a)): http://www.un.org/News/Press/docs/2001/sc7158.doc.htm. UN Security Council Resolution 1624 refers to the need to 'prevent terrorists from exploiting sophisticated technology, communications and resources' (14 September 2005, p.2): http://daccessdds.un.org/doc/UNDOC/GEN/N05/510/52/PDF/N0551052.pdf?OpenElement.

[60] UN Security Council Counter-Terrorism Committee: http://www.un.org/sc/ctc/index.html. See also UN Security Council, 'Report of the Counter-Terrorism Committee to the Security Council on the implementation of resolution 1624 (2005)' (S/2006/737, 15 September 2006), paras 6, 16, 43: http://daccessdds.un.org/doc/UNDOC/GEN/N06/520/37/PDF/N0652037.pdf?OpenElement.

[61] UN General Assembly, 'The United Nations Global Counter-Terrorism Strategy' (A/Res/60/288, 20 September 2006), paras 12(a), 12(b): http://daccessdds.un.org/doc/UNDOC/GEN/N05/504/88/PDF/N0550488.pdf?OpenElement.

[62] UN General Assembly, 'Creation of a global culture of cybersecurity', A/RES/57/239, 20th December 2002.

[63] 'Message for World Information Society Day: Secretary-General Calls for International Countermeasures to Enhance Cybersecurity', 17 May 2006, http://www.un.org/News/Press/docs/2006/sgsm10433.doc.htm.

Founded in Paris in 1865 as the International Telegraph Union, the ITU took its present name in 1934 and in 1947 became a specialized agency of the United Nations. Membership of the ITU includes all 191 countries which use the international telephone system, as well as almost 750 IT companies and other associates which are members of one or more ITU sectors.[64] The ITU's goals are ambitiously normative, as the organisation's mission statement indicates:

> ITU's mission is to enable the growth and sustained development of telecommunications and information networks, and to facilitate universal access so that people everywhere can participate in, and benefit from, the emerging information society and global economy. The ability to communicate freely is a pre-requisite for a more equitable, prosperous and peaceful world. And ITU assists in mobilizing the technical, financial and human resources needed to make this vision a reality.[65]

The ITU mission statement embraces the issue of cyber-security in direct terms. The organisation's goal is to develop 'confidence in the use of cyberspace through enhanced online security. Achieving cybersecurity and cyberpeace are amongst the most critical concerns of the information age, and ITU is taking concrete measures through its landmark Global Cybersecurity Agenda.'[66]

The ITU's **Global Cybersecurity Agenda** (GCA) was launched in 2007 as a framework for international cooperation. In a rather complicated arrangement, the GCA comprises five 'strategic pillars' (including legal and technical/procedural measures, organisation, capacity building and international co-operation) as well as seven 'main strategic goals' (ranging from cyber-crime legislation to software security and international digital identity protocols).[67] In September 2008 the ITU and the **International Multilateral Partnership Against Cyber-Threats** (IMPACT) entered into an agreement under which the GCA is to be co-located at IMPACT's headquarters in Cyberjaya, Malaysia.[68]

At the highest levels of the UN cyber-security is on the one hand associated directly with the challenge of terrorism, and on the other often described in 'soft' or 'cultural' terms – as a challenge to society as a whole. Within the ITU and its associated initiatives and programmes, there is clear evidence of a practical approach which bridges gaps between the worlds of public policy, technology and industry, and which assists in national capacity building.

Organisation for Economic Co-operation and Development

Drawn up in 2002 by the organisation's **Directorate for Science, Technology and Industry**, the OECD **Guidelines for the Security of Information Systems and Networks** have become something of a standard reference point for national and

---

[64] The ITU has three sectors: the Radiocommunication Sector (ITU-R); the Telecommunication Standardization Sector (ITU-T); and the Telecommunication Development Sector (ITU-D). In each of these sectors the ITU undertakes a range of technical, procedural and political measures related to cyber-security.

[65] ITU Mission: http://www.itu.int/net/about/mission.aspx.

[66] ITU Mission: http://www.itu.int/net/about/mission.aspx.

[67] Global Cybersecurity Agenda Strategic Pillars and Goals: http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html. A full account of the aims and activities of the GCA is available in the form of the GCA *Global Strategic Report* (Geneva: ITU, 2008): http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf

[68] Curbing Cyberthreats – IMPACT: http://www.itu.int/osg/csd/cybersecurity/gca/impact/index.html.

international cyber-security initiatives. The non-binding Guidelines have been adopted by 19 of the 30 OECD members and Brazil, and by the European Community. The Guidelines call for a participative approach to cyber-security, with governments, businesses and individuals all developing a 'greater awareness and understanding of security issues' and helping to create a 'culture of security', defined in the following terms:

> A focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks. The Guidelines signal a clear break with a time when secure design and use of networks and systems were too often afterthoughts.[69]

The Guidelines set out nine complementary principles upon which to organise and implement a culture of security:

1. **Awareness** [of the need for security of information systems];
2. **Responsibility** [of all participants for the security of information systems and networks];
3. **Response** [to security incidents should timely and co-operative];
4. Ethics [respect the legitimate interests of other users and promote best practice];
5. **Democracy** [security measures should be compatible with the essential values of democratic society];
6. **Risk assessment** [broad-based assessment of threats and vulnerabilities, as the basis for risk management];
7. **Security design and implementation** [security measures should be an essential feature of information systems and networks];
8. **Security management** [a comprehensive approach involving all participants on all levels, addressing threats as they emerge];
9. **Reassessment** [continual review, reassessment and modification of security measures as risks evolve].[70]

The OECD runs a website dedicated to the culture of security which, among many initiatives, provides links to 'security awareness tools' emerging around the world.[71] Other OECD cyber-security initiatives include a long series of downloadable reports on information security and privacy, including such subjects as national information security guidelines, OECD policy guidance on radio frequency identification, and cross-border enforcement of privacy laws;[72] an OECD 'privacy statement generator';[73] a set of 'resources on policy issues related to Internet governance', covering such areas as privacy, consumer protection and e-commerce;[74] and finally the Working Party on Information Security and Privacy, the goal of which is to provide 'a foundation for developing national coordinated policies.'[75]

---

[69] OECD, *Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security* (Paris: OECD, 25 July, 2002), p.8: http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.

[70] OECD, *Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security* (Paris: OECD, 25 July, 2002), pp. 9-12: http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.

[71] OECD Culture of Security: http://www.oecd.org/document/63/0,3343,en_21571361_36139259_36306559_1_1_1_1,00.html.

[72] OECD Reports on Information Security and Privacy: http://www.oecd.org/findDocument/0,3354,en_2649_34255_1_119666_1_1_1,00.html.

[73] OECD Privacy Statement Generator: http://www.oecd.org/document/39/0,3343,en_2649_34255_28863271_1_1_1_1,00.html.

[74] OECD Resources on Policy Issues Related to Internet Governance: http://www.oecd.org/document/21/0,3343,en_21571361_34590630_34591253_1_1_1_1,00.html.

[75] OECD Working Part on Information Security and Privacy: http://www.oecd.org/document/46/0,3343,en_2649_34255_36862382_1_1_1_1,00.html.

Encapsulated in the term 'culture of security', the OECD's approach to cyber-security can be summarised as largely facilitative: the development of internationally respected guidelines; the identification of best practice; and finally assistance in devising cyber-security policies and practices.

Organisation for Security and Co-operation in Europe

The OSCE has taken a growing interest in the challenge of cyber-security. In December 2004 the **Ministerial Council** (comprising the Foreign Ministers of OSCE participating states) resolved to address 'the extent of use of the Internet by terrorist organisations', including a range of activities such as terrorist recruiting, fund-raising, organisation and propaganda.[76] Two years later, Foreign Ministers called for enhanced international co-operation and for more effort to protect 'vital critical information infrastructures and networks against the threat of cyber attacks.' Participating states were urged to monitor more closely the websites of terrorist and extremist organisations, and to exchange information with other governments in the OSCE and other appropriate fora. In attempt to broaden participation in the general cyber-security effort, the Ministerial Council also called for 'more active engagement of civil society institutions and the private sector in preventing and countering the use of the Internet for terrorist purposes.'[77] The **Permanent Council** of the OSCE has also been a venue for debate and discussion concerning cyber-security.[78] In June 2008, for example, Estonian Defence Minister Jaak Aaviksoo spoke of an 'immense amount of work to be done' in the field of cyber-security.[79]

The OSCE's **Forum for Security Co-operation** (FSC) has also contributed to the organisation's involvement in the field of cyber-security. The FSC was founded in 1992 with a mandate to address military aspects of security within the OSCE area. The FSC's work has been concentrated largely on arms control, disarmament and confidence-building measures.[80] Latterly, however, the Forum has begun to take more of an interest in cyber-security. In October 2008 the FSC (in joint session with the Permanent Council), decided to convene an OSCE Workshop on a Comprehensive OSCE Approach to Enhancing Cyber Security in March 2009.[81] Finally, the OSCE has supported national efforts, such as the Armenian **Task Force on cyber-crime and cyber-security**.[82]

The OSCE has had a long-standing role in the pursuit of security and stability in Europe. Much of its past effort has been in the area of conventional weaponry and military holdings. As cyber-security has become a more prominent feature of European security in the early twenty-first century, so the OSCE has been adapting to the

---

[76] OSCE Ministerial Council Decision 3/04: Combating the Use of the Internet for Terrorist Purposes, 7 December 2004: http://www.osce.org/documents/mcs/2004/12/3906_en.pdf.
[77] OSCE Ministerial Council Decision 7/06: Countering the Use of the Internet for Terrorist Purposes, 5 December 2006: http://www.osce.org/documents/mcs/2006/12/22559_en.pdf.
[78] OSCE Permanent Council: http://www.osce.org/pc/.
[79] OSCE Permanent Council, 'OSCE can play important role in cyber security, says Estonian defence Minister', Vienna, 4 June 2008: http://www.osce.org/pc/item_1_31483.html.
[80] OSCE Forum for Security Co-operation: http://www.osce.org/fsc/.
[81] OSCE FSC/PC 36th Joint Meeting, FSC Decision No. 10/08, 'OSCE Workshop on a Comprehensive OSCE Approach to Enhancing Cyber Security', 29th October 2008: http://www.osce.org/fsc/.
[82] OSCE, 'OSCE office organises discussion in Yerevan on cyber security threats', 21 March 2006: http://www.osce.org/item/18450.html.

challenge and broadening its working agenda. In summary, the OSCE effort in cyber-security is still maturing, and could best be described as 'work in progress'.

Council of Europe

The Council of Europe's (COE) contribution to international cyber-security policy is in the form of the **Convention on Cybercrime**, which was opened for signature in November 2001 and which entered into force in July 2004. By 27 January 2009, 23 of the 47 member states of the COE (including Azerbaijan) had ratified the Convention (the most recent being Italy in October 2008); a further 19 member states had signed but not yet ratified the agreement (including Georgia and the United Kingdom); and five member states had not yet signed (including Russia). Three 'non-member states' of the COE had signed the Convention on its opening (Canada, Japan, South Africa), and one state had taken the process through to ratification (the United States ratified the Convention in September 2006 and the Convention entered into force in the United States in January 2007).[83] Sixteen other non-COE countries were reported as 'known to use the Convention as a guideline for their national legislation' (including Brazil and India).[84]

Directed at 'terrorist groups, pornographers and paedophile networks, illegal traffickers in weapons, drugs and human beings, money launderers and cybercriminals',[85] the Cybercrime Convention, like other international initiatives reviewed here, has a facilitative and advisory function, providing 'guidelines for all governments wishing to develop legislation against cybercrime' in pursuit of closer co-ordination of national efforts. The distinctive feature of the Convention, however, is that it is much more than advisory: the Council of Europe describes the convention as 'the only binding international treaty on the subject to have been effectuated to date.'[86] The Convention details the crimes and offences which signatory governments should bring into domestic law and implement, ranging from illegal interception of data, to computer-related fraud, and offences related to child pornography. [Articles 2-11] Elsewhere, the Convention sets out procedures by which computer data can be restored and retrieved for the purposes of criminal investigation [Articles 16-21], and by which the signatories to the Convention 'shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence'. Under the Convention, mutual assistance requires each signatory to have a designated point of contact available on a '24/7' basis. [Articles 25-35][87]

The Council of Europe Convention on Cybercrime is significant in several respects. First, the Convention addresses illegal activities and practices which feature across the spectrum of cyber-security threats. Second, the Convention establishes common standards and procedures which are legally binding on its signatories. Third, the

[83] Council of Europe Convention on Cybercrime: http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.
[84] Council of Europe, 'Global reach of the Council of Europe Convention on Cybercrime': http://www.coe.int/t/dc/files/themes/cybercrime/WorldMapCybercrime_E_2008_10_06.pdf.
[85] An additional protocol to the Convention also forbids 'acts of a racist and xenophobic nature committed through computer systems'.
[86] Council of Europe, 'Cybercrime: a threat to democracy, human rights and the rule of law': http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp.
[87] Council of Europe, Convention on Cybercrime (Budapest, 23 November 2001: Council of Europe Treaty Series No. 185): http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

Convention is open to Council of Europe member states and others, thereby increasing its authority as an international instrument. Finally, the Convention introduces requirements for data handling and access which have given rise to concerns over privacy law and civil liberties.

North Atlantic Treaty Organisation

As a sophisticated politico-military alliance, NATO has long been familiar with the use of, and defence against electronic and information warfare. For a number of years NATO has been closely involved in the US-led efforts to 'transform' military organisation and the conduct of operations through 'network-centric warfare' and 'network-enabled capability'. At the Prague Summit in November 2002 NATO leaders resolved to 'strengthen our capabilities to defence against cyber attacks'.[88] The Prague decision resulted in a range of initiatives. A new NATO **Cyber-Defence Programme** was initiated, involving various NATO bodies: the **NATO Communication and Information Systems Services Agency** (NCSA), described as the Alliance's 'first line of defence against cyber terrorism'; the **NATO Information Security Technical Centre** (NITC), responsible for communications and computer security; the **NATO Information Security Operations Centre**, responsible for the management of cryptographic equipment and the co-ordination of responses to cyber attacks against NATO; and the **NATO Computer Incident Response Capability** (NCIRC), tasked with the protection of NATO's encrypted communications and systems.[89]

Following the cyber-attacks against Estonia in April and May 2007, NATO ministers agreed the outlines of an Alliance-wide cyber-defence concept at Nordwijk in October 2007,[90] and this in turn developed into the NATO **Policy on Cyber-Defence** agreed in early 2008.[91] The policy was described at the Alliance's April 2008 Bucharest Summit in the following terms:

> We have recently adopted a Policy on Cyber Defence, and are developing the structures and authorities to carry it out. Our Policy on Cyber Defence emphasises the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack. We look forward to continuing the development of NATO's cyber defence capabilities and strengthening the linkages between NATO and national authorities.[92]

Following the Bucharest Summit the NATO **Cyber-Defence Management Authority** (CDMA) was created in order to bring together 'the key actors in NATO's cyber defence activities. The Authority will manage cyber defence across all NATO's communication and information systems and could support individual Allies in defending against cyber attacks upon request.'[93] At about the same time, Alliance

---

[88] NATO Prague Summit Declaration Article 4(f), 21 November 2002: http://www.nato.int/docu/pr/2002/p02-127e.htm.
[89] NATO Communication and Information Systems Services Agency: http://www.ncsa.nato.int/topics/combating_cyber_terrorism.htm.
[90] European Security and Defence Assembly, 'Cyber warfare' (Assembly of the Western European Union, Defence Committee Report C/2022. 5 November 2008), p.19.
[91] NATO, 'Defence against cyber attacks', 26 June 2008: http://www.nato.int/issues/cyber_defence/index.html.
[92] NATO, Bucharest Summit Declaration, Art. 47, 3 April 2008: http://www.nato.int/docu/pr/2008/p08-049e.html.
[93] NATO, 'Defending against cyber attacks: what does this mean in practice?', 31 March 2008: http://www.nato.int/issues/cyber_defence/practice.html.

leaders agreed to the formal establishment of the **NATO Co-operative Cyber Defence Centre of Excellence** (CCD-CoE) which had been under development since 2004. Based in Tallinn, the significance of the CCD-CoE was emphasised in the attacks on Estonia in 2007, and in October 2008 NATO's North Atlantic Council granted the CCD-CoE full NATO accreditation and the status of International Military Organisation.[94] In the words of Estonia's Defence Minister Kaak Aaviksoo, however, the CCD-CoE does *not* have military aims as such, but is a facility for 'expertise, scientific research and development, where the nature and various means of cyber attacks that have been used can be studied.'[95] The 'mission and vision' of the CCD-CoE are described as follows: 'to enhance the cooperative cyber defence capability of NATO and NATO nations, thus improving the Alliance's interoperability in the field of cooperative cyber defence' and to be 'a primary source of subject matter expertise for NATO in cooperative cyber defence related matters.'[96] The CCD-CoE's core research areas include the following: Doctrine and concept development; Awareness and training; Research and development; Analysis and lessons learned; and Consultation.[97] The organisation has seven 'Sponsoring Nations': Estonia, Germany, Italy, Latvia, Lithuania, Slovak Republic and Spain. In November 2008 the United States agreed to become a Sponsoring Nation and Turkey announced its intention to do the same. Membership of the CCD-CoE is open to all NATO nations, while non-members of NATO, universities, research institutions and businesses may join as 'Contributing Participants'.

NATO is a politico-military alliance of long-standing. Yet the breadth and complexity of NATO's work in cyber-security indicates that the Alliance does not regard cyber-security and cyber-defence in traditional military and defence terms. NATO is able to combine political, military, industrial and technological approaches to cyber-security, and through initiatives such as the CCD-CoE is able to develop international best practice with contributions from non-NATO governments and other interested parties.

Group of Eight

The G8's principal contribution to international cyber-security policy is the **Sub-Group on High-Tech Crime**, founded as a sub-group of the 1996 Lyon Group to combat transnational organised crime. The goal of the sub-group was to 'enhance the abilities of G8 countries to prevent, investigate, and prosecute crimes involving computers, networked communications, and other new technologies.' The mission of the sub-group was later broadened to include terrorist uses of the Internet and protection of critical information infrastructures.[98] The sub-group seeks to deal with cyber-crime not only within the jurisdiction of G8 countries but also to create guidelines which other countries might choose to implement. The sub-group has created a **24/7 Network of Contacts for High-Tech Crime** as well as an international **Critical Information Infrastructure Protection (CIIP) Directory**. The sub-group has published best

[94] CCD-CoE, 'History and way ahead': http://www.ccdcoe.org/12.html.
[95] OSCE Permanent Council Press Release, 'OSCE can play important role in cyber security, says Estonian Defence Minister', 4 June 2008: http://www.osce.org/pc/item_1_31483.html.
[96] CCD-CoE, 'Mission and Vision': http://www.ccdcoe.org/11.html.
[97] CCD-CoE, 'Core areas': http://www.ccdcoe.org/37.html.
[98] Meeting of G8 Justice and Home Affairs Ministers, G8 Sea Island Summit, 11 May 2004: http://www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html.

practice documents and guides for computer and network security threat assessments, and has organised international training conferences for cyber-crime agencies.[99]

Summary: Part 2

This brief survey shows how different international organisations have responded to the cyber-security challenge. It is to be expected that an organisation will bring with it a certain amount of 'baggage' as it approaches new and evolving threats. NATO, for example, is a long-standing politico-military organisation; an experience which colours its understanding and management of cyber-security. But it is striking that in each case surveyed here, the organisation in question appears to have recognised the breadth and complexity of the cyber-security challenge and has sought neither to redefine the problem in its own exclusive terms, nor to act as if in a closed system. On empirical grounds, therefore, we can say that the response to the cyber-security challenge is developing along multi-organisational lines, and it appears suitable that this should be the case. It is also clear that while governments are, clearly, the most important actors in cyber-security, others have a contribution to make, including industry and the private commercial sector. Within each organisation there are various judgements to be made. In seeking the security of the organisation, its members and affiliates, and their interests, there is a balance to be struck between defensive/passive/protective measures, and a more activist or offensive stance. Then there is a balance to be struck between security measures (of whatever sort) and civil liberties. And finally, there is a balance to be struck between securing the specific interests of a given organisation or government, and the more general requirement to create, for the benefit of all legitimate users, an international communications and technological environment which is as hostile as possible to the activities and ambitions of cyber-terrorists and extremists, cyber-criminals and hackers.

PART 3: THE EUROPEAN UNION, CYBER-SECURITY AND THE COMMON FOREIGN AND SECURITY POLICY

The third part of the paper has three tasks: first, to outline European Union (EU) approaches and initiatives in cyber-security; second, to explore the connection between cyber-security and the Common Foreign and Security Policy; and finally to examine the feasibility of an EU Cyber-Security Co-ordinator.

European Union Initiatives in Cyber-Security[100]

There can be no doubt that the European Union (EU) has been vigorous in its response to the challenge of cyber-security, with various EU bodies and agencies being responsible for a wide variety of initiatives. At the declaratory level the **European Commission** has taken a leading role in articulating policy responses at several points on the cyber-security spectrum. Thus, in 2001 the Commission published a Communication on information society which warned that 'Information and communication infrastructures […] have their own vulnerabilities and offer new

[99] Cyber Security Organization Catalog, 'Group of Eight (G8)': http://www.cistp.gatech.edu/catalog/oneOrg.php?id=3.

[100] A complete account of the very extensive range of EU cyber-security activities is not possible in the space available here. For a more comprehensive assessment see Cyber Security Organization Catalog, 'European Union (EU)', 9 November 2008: http://www.cistp.gatech.edu/catalog/oneOrg.php?id=7.

opportunities for criminal conduct,'[101] and in 2006 addressed the problem of spam, spyware and malware.[102] In 2006 the Commission proposed a 'Strategy for a Secure Information Society' which called for a 'multi-stakeholder approach' to information security and for the further development of a 'dynamic, global strategy in Europe, based on a culture of security and founded *on dialogue, partnership and empowerment*.'[103] The Commission is also engaged with lower-level cyber-security challenges. With a budget of €55 million for 2009-2013, the Commission's **Information Society and Media Directorate-General** hosts a 'Safer Internet plus' programme intended to 'protect online environments from illegal and harmful online content, which ranges from racism and bullying to child pornography and child grooming.'[104]

Most recently, in November 2008 the Commission launched a public consultation exercise on network and information security policy in Europe. Describing the ICT infrastructure as 'the nervous system of our modern society', the Commission argued that 'network and information security challenges will require a strong, coordinated European response. Recent cyber-attacks targeting individual countries have shown that one country on its own can be very vulnerable.' By early January 2009 the Commission hoped to receive responses from as many 'stakeholders' as possible 'on the possible objectives for a strengthened network and information security policy at EU level and on the means to achieve those objectives.'[105]

Under the auspices of the EU's inter-governmental Third Pillar – **Police and Judicial Co-operation** (PJC) – cyber-security is addressed in a more direct and operational manner in the contexts of terrorism, organised crime and financial crime. At the operational level, for example, the **European Police Office** (EUROPOL), an agency of the PJC, produces an annual *EU Terrorism Situation and Trend Report*, the 2008 edition of which notes the extensive use of the Internet for a wide range of terrorist purposes.[106] At the strategic level, the EU's December 2005 **Counter-Terrorism Strategy** acknowledges the significance of the ICT infrastructure in each of its four work strands – Prevent, Protect, Pursue, Respond.[107]

---

[101] Commission of the European Communities, 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime', COM (2000) 890 Final, 6 January 2001: http://ec.europa.eu/archives/ISPO/eif/InternetPoliciesSite/Crime/CrimeComEN.pdf.

[102] Commission of the European Communities, 'On Fighting spam, spyware and malicious software', COM (2006) 688 Final, 15 November 2006: http://ec.europa.eu/information_society/policy/ecomm/doc/info_centre/communic_reports/spam/com_2006_0688_f_en_acte.pdf.

[103] Commission of the European Communities, 'A Strategy for a Secure Information Society: "Dialogue, Partnership and Empowerment"', COM (2006) 251 Final, 31 May 2006: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:EN:PDF. [Emphasis in original]

[104] European Commission, Information Society and Media DG, 'Making the Internet a safer place', June 2008: http://ec.europa.eu/information_society/doc/factsheets/018-saferinternetplus-en.pdf.

[105] European Commission: Information Society Portal, 'Public consultation on network and information security', 7 November 2008: http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=4464.

[106] European Police Office, *EU Terrorism Situation and Trend Report 2008* (The Hague, 2008): http://www.europol.europa.eu/publications/EU_Terrorism_Situation_and_Trend_Report_TE-SAT/TESAT2008.pdf.

[107] Council of the European Union, 'The EU Counter-terrorism Strategy' (14469/4/05, 30 November 2005): http://register.consilium.europa.eu/pdf/en/05/st14/st14469-re04.en05.pdf.

The **European Parliament** takes an interest in the information society and cyber-security through the work of several of its standing committees. The Committee on Industry, Research and Technology (ITRE) concerns itself, inter alia, with 'the information society and information technology, including the establishment and development of trans-European networks in the telecommunication infrastructure sector.'[108] The Committee on Civil Liberties, Justice and Home Affairs (LIBE) has oversight of 'legislation in the areas of transparency and of the protection of natural persons with regard to the processing of personal data,'[109] and the Committee on Culture and Education (CULT) addresses 'audiovisual policy and the cultural and educational aspects of the information society'.[110] Finally, the Committee on Foreign Affairs (AFET) has responsibility for regional and international security and for the Common Foreign and Security Policy.[111]

The EU has also taken a number of agency-level initiatives. In February 2002 the Commission established the **Contact Network of Spam Authorities**,[112] an initiative in which, according to StopSpamAlliance.org, 'information on current practices to fight spam is exchanged between national authorities, including best practices for receiving and handling complaint information and intelligence and investigating and countering spam.'[113] The core tasks of the **European Network and Information Security Agency** (ENISA), established in 2004, are set out in its General Information Security Strategy: 'raising awareness for information security issues and the promotion of best practices in the field of network and information security.'[114] Article 2 of the regulation establishing ENISA is more specific as to the goals of the Agency: to 'enhance 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.'[115]

ENISA describes itself as a 'Centre of Excellence' (and 'Expertise') in information security. Like NATO's CCD Centre of Excellence in Tallin, ENISA is also based at some distance from Brussels – in Crete. For some critics, the choice of location is but one of many problems confronting ENISA. Across the EU there are very different levels of experience and understanding of information security and cyber-security, suggesting that there might be insufficient common ground upon which ENISA could construct a credible work programme. At the national level, important differences remain in the implementation of information security law, and it is not clear that ENISA

---

[108] European Parliament, ITRE Committee: http://www.europarl.europa.eu/activities/committees/homeCom.do?language=EN&body=ITRE.
[109] European Parliament, LIBE Committee: http://www.europarl.europa.eu/activities/committees/homeCom.do?language=EN&body=LIBE.
[110] European Parliament, CULT Committee: http://www.europarl.europa.eu/activities/committees/homeCom.do?language=EN&body=CULT.
[111] European Parliament, AFET Committee: http://www.europarl.europa.eu/activities/committees/homeCom.do?language=EN&body=AFET.
[112] Europa Press Releases, 'European countries launch joint drive to combat 'spam'' (Brussels, IP/05/146, 7 February 2005): http://europa.eu/rapid/pressReleasesAction.do?reference=IP/05/146.
[113] StopSpamAlliance.org, 'The EU Contact Network of Spam Authorities': http://stopspamalliance.org/?page_id=11.
[114] ENISA, 'General Information Security Strategy' (ENISA/TD/AP/D(2006) 136, 6 April 2006): http://www.enisa.europa.eu/pages/Security%20Strategy.html.
[115] Official Journal of the European Union, 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: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:077:0001:0011:EN:PDF.

will be able to overcome these differences. For example, in spite of efforts to harmonise electronic signature law across the EU for the sake of a 'level playing field' in e-commerce, certain governments have implemented their own legal mechanisms, thereby undermining the EU-wide approach. ENISA also has aspirations to work in sensitive areas of security policy (such as the protection of critical national infrastructure) for which they require access to national procedures, key individuals, databases etc. Yet these are often precisely the areas where national authorities are most reluctant to release information, least of all to a small international body far from sight, which might be thought to be unable to guarantee the security of the information it receives.

It is difficult to identify an EU body or agency which does *not* have some interest or involvement in cyber-security concepts and policy on the one hand, and/or in delivery and operations on the other. It should also be borne in mind that each of the EU's 27 national governments is engaged with the problem of security, at one level or another. It is also difficult to find an aspect of the cyber-security challenge which has not been addressed within the EU, broadly defined: information, computer and network security; the security of private individuals (including children); banking fraud and identity theft; organised criminality and the use of ICT by extremists; regulation; civil liberties, freedom of speech and data protection; e-commerce, innovation and the protection of high-tech intellectual property; critical infrastructure protection; the importance of an open ICT infrastructure for European culture and the media. All these areas, and others, have been addressed in one way or another. Yet for all the vigour and diversity of the EU's response to the cyber-security challenge, what is notably absent is a single strategy for cyber-security, uniting all EU efforts into one. In a relatively brief passage covering cyber-security, the 2008 report on the implementation of the EU's security strategy makes this point succinctly: 'More work is required in this area, to explore a comprehensive EU approach, raise awareness and enhance international co-operation.'[116] But how might a 'comprehensive EU approach' be achieved, and by whom (or what)?

Cyber-Security and the Common Foreign and Security Policy

Should the EU's Pillar II – the inter-governmental Common Foreign and Security Policy – have a more prominent (and perhaps co-ordinating) role in cyber-security? This question began to be answered by 9/11 and by the series of terrorist incidents in Europe in subsequent years. As a result of these events it became progressively more difficult to argue both that the CFSP was a sufficient response to the EU's security needs and that security policy could be the exclusive concern of EU national governments. The CFSP would not, of course, lose its position at the centre of the EU's security framework, but it would be complemented by other agencies and interests. It also became more difficult to argue that the CFSP should, somehow, be primarily outward facing and less concerned with the 'domestic' security of the EU, its member states and institutions. A more multilateral approach to European security was made explicit in the EU Counter-Terrorism Action Plan, published in late September 2001, which not only called for 'co-operation with the US' and referred to the EU's

[116] Report on the Implementation of the European Security Strategy: Providing Security in a Changing World' (Brussels, 11 December 2008, S407/08), p.5: http://www.eu-un.europa.eu/documents/en/081211_EU%20Security%20Strategy.pdf.

'involvement in the world,' but also emphasised the merits of co-operation between the institutions and EU Member States.[117]

The argument for multilateralism was taken further by the 2003 European Security Strategy which insisted that 'In a world of global threats, global markets and global media, our security and prosperity increasingly depend on an effective multilateral system. The development of a stronger international society, well functioning international institutions and a rule-based international order is our objective.'[118] In other words, counter-terrorism should be an international effort in which the strengths of international institutions as well as national governments are all exploited to the general benefit. By 2007 the EU's language had become stronger still. The EU Terrorism Situation and Trend Report (TE-SAT), published for first time in 2007, argued that 'The EU as a political institution is increasingly being identified as a symbol and has already become *threatened and targeted by terrorists*.'[119]

As a result of the recent encounter with terrorism, the EU's CFSP has been increasingly internationalised, while within the EU it has been recognised that the CFSP should be but one component of an inter-agency, comprehensive response to security challenges made against the EU. What the terrorist outrages have also done, to a very considerable extent, is dissolve the boundary between 'foreign' and 'domestic' security concerns. Albeit in response to terrorism, these shifts in the character of the CFSP have meant that the EU's Pillar II is now, arguably, in an inescapably appropriate condition to deal with the challenges of cyber-security, and arguably to assume a co-ordinating function. The range of threats described in Part 1, and the interdependence of these threats, should defeat any notion that cyber-security is divisible: between foreign and domestic; between military and civil; and between governments and other inter-governmental or indeed non-governmental actors. Furthermore, just as terrorism has become more real than theoretical for the EU, so too has cyber-security ceased to be an optional agenda item for any organisation which is western, wealthy and cyber-dependent. As a recent report on 'cyber warfare' by the European Security and Defence Assembly argues:

> National entities and governmental and non-governmental organisations also use the Internet for communication and information purposes. These institutional players are therefore vulnerable to cyber attacks aimed at objectives as numerous and varied as the motives and interests of the attackers themselves: disruption, disinformation, detection of vulnerable points, exaggeration or propaganda, for example.[120]

A *prima facie* argument can be made for a CFSP involvement in cyber-security. Nevertheless, it is clear that CFSP cannot be sufficient as the EU's response to cyber-security. One way to produce a fully synthesised, comprehensive approach to cyber-security would be to prepare a binding, EU-wide comprehensive strategy, or perhaps even to collapse all cyber-relevant bodies and agencies of the EU and its member states into one new, monolithic structure for cyber-security. But even a passing acquaintance

---

[117] European Council, 'Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001', pp.1-5: http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/ec/140.en.pdf.
[118] European Security Strategy, 'A Secure Europe in a Better World' (Brussels, 12 December 2003), p.9: http://consilium.europa.eu/uedocs/cmsUpload/78367.pdf.
[119] European Police Office, *EU Terrorism Situation and Trend Report 2007* (The Hague, 2007), p.36: http://www.europol.europa.eu/publications/EU_Terrorism_Situation_and_Trend_Report_TE-SAT/TESAT2007.pdf. [Emphasis added]
[120] European Security and Defence Assembly, 'Cyber warfare', p.10

with the history and structure of the EU would suggest these to be ambitious ideas. A cross-cutting strategy would probably not be able to reflect the myriad cyber-security interests without making controversial compromises for the sake of clarity and organisational efficiency, and would in any case be regarded as inappropriately hierarchical. And it is also unlikely that member states would contemplate being 'synthesised' with equanimity. Furthermore, it would be a strategic error and counter-productive to attempt to organise the EU's response in this way. The challenge of cyber-security is complex and dynamic and the response to that challenge should be flexible and responsive, drawing upon the widest range of experience and expertise available among the member states, institutions and agencies of the EU. The complex challenge of cyber-security requires a complex response. The diversity of the EU's responses to the cyber-security challenge should be regarded as a strength, rather than a weakness, but only insofar as those responses can be co-ordinated and deconflicted, and only insofar as the various bodies, agencies and governments of the EU can adopt a common operating vision for cyber-security. Rather than pursue a centrally disciplined, unified approach to cyber-security, what would be more appropriate – both for the EU and for the nature of the cyber-security challenge – would be an approach which might be described as *comprehensiveness in diversity*, and which should be achieved by co-ordination.

European Union Cyber-Security Co-ordinator

Following the terrorist attacks in Madrid in March 2004, the European Council agreed to the appointment of a Counter-Terrorism Co-ordinator. Recognising that a 'comprehensive and strongly coordinated approach is required in response to the threat posed by terrorism', the European Council set out the mandate for the new post in the following terms:

> The Co-ordinator, who will work within the Council Secretariat, will co-ordinate the work of the Council in combating terrorism and, with due regard to the responsibilities of the Commission, maintain an overview of all the instruments at the Union's disposal with a view to regular reporting to the Council and effective follow-up of Council decisions.[121]

A detailed review of the roles, responsibilities and achievements of the Counter-Terrorism Co-ordinator is not necessary for the purposes of this paper. What can be said, however, is that a precedent clearly exists for the appointment of a co-ordinator in an area of security policy which is not only complex and evolving, but which also crosses intra-EU boundaries. The appointment of a European Union Cyber-Security Co-ordinator (CSC) would have a number of advantages. In the first place, the appointment would adopt a model which is tried and tested and which is generally understood within the EU. Second, a CSC would act as a Brussels-based policy focal point, both within the EU and internationally. Finally, based in the Council Secretariat, the CSC would be in a strong position to liaise between the cyber-security efforts of the institutions and agencies of the EU, and those of member states. A provisional list of the roles and responsibilities of the Cyber-Security Co-ordinator might include the following:

1. Review of threats and vulnerabilities. On a regular basis, the CSC would review cyber-security threats to the EU and the level of vulnerability to those threats.

[121] European Council, 'Declaration on Combating Terrorism' (Brussels, 25 March 2004), para. 14: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/79637.pdf.

2. Information sharing. Information and analysis of threats and vulnerabilities would be shared across the EU and its member governments, in order to lay the foundations of a shared perception of threat and vulnerability, and to prevent the development of closed system approaches to cyber-security.
3. Review of structures, activities and initiatives. The first step towards co-ordination is deconfliction. With so many EU institutions, agencies and governments making some effort in cyber-security, it would be valuable to record those initiatives centrally and distribute the record to all interested parties.
4. Best practice. As different approaches to cyber-security are collated, it should be a straightforward step to identify best practice and to distribute 'lessons learned' accordingly.
5. Member states. By acting as a neutral conduit for information, analysis and best practice, the CSC would serve a key function in raising cyber-security standards among the member states of the EU.
6. Risk management. Through the distribution of information, analysis and best practice, the CSC would introduce a culture of prioritisation and mutually supportive risk management.
7. Research and innovation. Working in conjunction with ENISA, the CSC could act as a conduit for ICT and cyber-security innovation, relevant to the needs of the EU.
8. Security, defence and military. Based in the Council Secretariat, the CSC would be in a strong position to liaise with the instruments of the European Security and Defence Policy and the European Defence Agency, where the work of these bodies is relevant to cyber-security.
9. Common vision. The CSC would be responsible for the production and updating of an EU *Common Operating Vision for Cyber-Security*. This 'living' document would function at the operational, rather than the strategic level, seeking to achieve operational consistency across the EU.
10. Point of contact. The CSC would serve as a point of contact with non-EU governments and other international organisations and bodies, and would represent the EU's work in cyber-security. In addition, the CSC would be the point of contact for urgent technological requirements and procurement, and for the general public. The office of the CSC could distribute public cyber-security warnings across the EU.

Summary: Part 3

In its various forms, the EU is very closely engaged in cyber-security. The EU cannot, however, be said to have a comprehensive approach to cyber-security; the EU's responses are diverse, lack coherence and could at times conflict. There is some irony in this, in that the European Union is a vast undertaking in government and administration which touches upon most conceivable aspects of societal, commercial and private life. Yet the EU appears unable to organise a comprehensive approach to cyber-security challenges which, if taken together, could be said to threaten the EU comprehensively. In broad terms, a more coherent approach could be achieved in one of two ways: either by uniting the EU's cyber-security efforts around one central strategy (and perhaps even within a new institutional framework); or by seeking a more efficient co-ordination of effort, while maintaining institutional and role specialisations. The latter approach is preferable; a co-ordinated approach reflects more closely the politics and structures of the EU and would be more responsive to the complex and evolving challenge of cyber-security. *Comprehensiveness in diversity* calls, in the first

place, for a more prominent role for the Common Foreign and Security Policy and for the establishment within the Council Secretariat of a Cyber-Security Co-ordinator.

CONCLUSION AND RECOMMENDATIONS

The European faces a broad range of cyber-threats including hacking, serious and organised crime, ideological and political extremism, and state-sponsored cyber-aggression. While these different threats do not constitute a vast cyber-conspiracy against the EU, there is no doubt that the EU is challenged comprehensively – and even systemically – by this range of threats. In Part 2 several international organisations were examined for the style of their response to the challenge of cyber-security. It is clear that no one organisation can offer a complete solution to the problem of cyber-security, and that all approaches are essential if the global ICT infrastructure is to be made as inhospitable as possible for criminals and extremists. Precisely the same judgement can be made of the EU. The institutions, agencies and governments of the EU all contribute in different ways to meeting the cyber-security challenge. The question then is how to combine these efforts more efficiently and comprehensively, without compromising the experience and expertise available within the EU, and while acknowledging the character of the EU? Describing the preferred approach as *Comprehensiveness in Diversity*, Part 3 concluded by recommending a more distinctive role for the Common Foreign and Security Policy, and the establishment of a Cyber-Security Co-ordinator.

In summary, this paper makes the following **recommendations:**

1. There should be no attempt at a centralised, unified, cross-cutting approach to cyber-security within the EU. Such an approach would conflict with the political character and bureaucratic structures of the EU, resulting in a loss of flexibility and a narrowing of the EU's response to the ever-widening challenge of cyber-security.
2. The EU should adopt a policy described as *Comprehensiveness in Diversity* (or in similar language) with the following three aims:
    a. Establish a clear role within the overall cyber-security response for the EU's Common Foreign and Security Policy. Uniquely within the EU, the CFSP will be able to bridge the civil-military divide where cyber-security is concerned, and will connect the internal and external aspects of cyber-security.
    b. Establish the post of Cyber-Security Co-ordinator with the Council Secretariat, acting in close liaison with EU institutions and member governments, and with relevant agencies such as ENISA, ESDP and EDA.
    c. Prepare a Common Operating Vision for cyber-security. Emphatically not a strategic document, the Common Operating Vision would seek to achieve operational consistency across the EU.

SELECT BIBLIOGRAPHY

- Brenner, S.W., 'Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships', *North Carolina Journal of Law & Technology* (Vol.4, Issue 1, Fall 2002).
- British-North America Committee, *Cyber Attack: A Risk Management Primer for CEOs and Directors* (BNAC, 2007).
- Choo, K.R. and R. G. Smith, 'Criminal Exploitation of Online Systems by Organised Crime Groups', *Asian Criminology* (Vol. 3, No. 1, June 2008).
- Cornish, P., R. Hughes and D. Livingstone, *Cyber-space and the national security of the United Kingdom* (London: Chatham House, forthcoming 2009).
- Emigh, E., 'Terror on the Internet', *Government Security* (1 October 2004), http://govtsecurity.com/federal_homeland_security/terror_internet/
- European Police Office, *EU Terrorism Situation and Trend Report 2007* (The Hague, 2007), http://www.europol.europa.eu/publications/EU_Terrorism_Situation_and_Trend_Report_TE-SAT/TESAT2007.pdf
- European Police Office, *EU Terrorism Situation and Trend Report 2008* (The Hague, 2008), http://www.europol.europa.eu/publications/EU_Terrorism_Situation_and_Trend_Report_TE-SAT/TESAT2008.pdf
- European Security and Defence Assembly, 'Cyber warfare' (Assembly of the Western European Union, Defence Committee Report C/2022. 5 November 2008).
- Fafinski, S. and N. Minassian, *UK Cybercrime Report 2008* (Garlik, September 2008), http://www.garlik.com/static_pdfs/cybercrime_report_2008.pdf
- Fickes, M., 'Cyber Terror', *Government Security* (1 July 2008), http://www.govtsecurity.com/federal_homeland_security/cyber_terror_attacks/index.html
- Kahl, C.H., 'COIN of the Realm: Is There a Future for Counterinsurgency?', *Foreign Affairs* (86/6, November/December 2007).
- Kimmage, D., *The Al-Qaeda Media Nexus: The Virtual Network Behind the Global Message* (Washington DC: RFE/RL Special Report, 2008).
- Metz, S., *Rethinking Insurgency* (Carlisle: US Army War College Strategic Studies Institute, June 2007).
- Microsoft, *Security Intelligence Report* (Key Findings Summary: January through June 2008), http://www.microsoft.com/security/portal/sir.aspx
- Negroponte, N., *Being Digital* (New York: Vintage Books, 1996).
- Reilly, M., 'When nations go to cyberwar', *New Scientist*, 23 February 2008.
- Stenersen, A., 'The Internet: A Virtual Training Camp?', *Terrorism and Political Violence* (Vol. 20, 2008).
- 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
- 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