

Global Project on Cybercrime
www.coe.int/cybercrime



COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version 14 October 2011
Strasbourg, France

Draft / Work in progress

Discussion paper

Cybercrime Strategies

Prepared by
Global Project on Cybercrime

**Project funded by Estonia, Japan, Monaco, Romania, Microsoft, McAfee, Visa Europe
and the Council of Europe**

Work in progress

This report is based on a discussion paper prepared by Alexander Seger (Council of Europe) for Workshop 115 at the Internet Governance Forum in Nairobi, Kenya, on 28 September 2011. It had received comments prior to that workshop from Markko Künnapu (Estonia), Monika Josi, Roger Halbheer and Jean-Christophe Le Toquin (Microsoft), Zahid Jamil (Pakistan), Cristina Schulman (Council of Europe).

Panellists in the workshop included Markko Künnapu (Estonia), Christopher Painter (USA), Jayantha Fernando (Sri Lanka), Andrew Cushman (Microsoft), Bill Smith (PayPal) and Zahid Jamil (Pakistan). Many of the 90 participants intervened in the discussion.

The present version takes into account comments made during that workshop.

Discussions are to continue at the Octopus Conference on Cooperation against Cybercrime (Strasbourg, 21-23 November 2011) www.coe.int/octopus

Please provide feedback to alexander.seger@coe.int

For further information please contact:

Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe
Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Disclaimer:

This technical report does not necessarily reflect official positions of the Council of Europe or of the donors funding this project or of the parties to treaties referred to.

Contents

1	Introduction	4
2	Cybercrime and cybersecurity: current concepts and strategies	6
2.1	Cybersecurity	6
2.2	Cybercrime	7
3	Cybercrime policies and strategies: possible elements	12
3.1	Scope of a cybercrime strategy	12
3.2	Objective of a cybercrime strategy	13
3.3	Measures	13
3.3.1	Cybercrime reporting and intelligence	13
3.3.2	Prevention	13
3.3.3	Legislation	13
3.3.4	High-tech crime and other specialised units	14
3.3.5	Interagency cooperation	14
3.3.6	Law enforcement training	14
3.3.7	Judicial training	14
3.3.8	Public/private (LEA/ISP) cooperation	15
3.3.9	Effective international cooperation	15
3.3.10	Financial investigations and prevention of fraud and money laundering	15
3.3.11	Protection of children	16
3.4	Responsibilities for management, coordination, implementation, monitoring	16
3.5	Technical assistance for capacity building	16
4	Cybercrime and cybersecurity strategies: complementarity	17
5	Conclusion	19
6	Appendix: Examples of cybersecurity and cybercrime strategies	21
7	References	32

1 Introduction

The security of information and communication technology (ICT) as well as the question of cybercrime have been of concern for some time.¹ However, it was only in the recent past, that governments began to understand the significance of ICT security for societies that are being transformed by technology and that have become reliant on computer networks. The security of ICT is thus becoming a policy priority of many governments.

The 2007 attacks on Estonia² were instrumental in this respect. Many countries responded by adopting cybersecurity strategies. For example:

- Australia – Attorney General Department (2009): Cyber Security Strategy³
- Canada (2010): Canada’s Cyber security Strategy⁴
- Czech Republic (2011): Cyber Security Strategy for the Czech Republic for the 2011 – 2015 Period⁵
- Estonia – Ministry of Defence (2008): Cyber Security Strategy⁶
- France – Agence Nationale de la Sécurité des Systems d’Information (2011): Défense et sécurité des systèmes d’information – Stratégie de la France⁷
- Germany – Federal Ministry of the Interior (2011): Cyber Security Strategy for Germany⁸
- Netherlands (2011): The National Cyber Security Strategy (NCSS)⁹
- United Kingdom – Cabinet Office (2009): Cyber Security Strategy for the United Kingdom¹⁰

Other countries, such as India¹¹ or South Africa¹², are in the process of developing similar strategies or policies.¹³

¹ For example, the first Computer Emergency Response Team (CERT) was created in 1988 at Carnegie Mellon University; in 1989 the Council of Europe (Committee of Ministers) adopted recommendation R(89)9 on computer-related crime; in the 1990s many governments began to adopt legislation on cybercrime or electronic crime; in 2001, the Council of Europe adopted the Budapest Convention on Cybercrime; in 2002, the OECD adopted “Guidelines for the Security of Information Systems and Networks” etc.

² http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

³

[http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/\(4CA02151F94FFB778ADAEC2E6EA8653D\)~AG+Cyber+Security+Strategy+-+for+website.pdf/\\$file/AG+Cyber+Security+Strategy+-+for+website.pdf](http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf)

⁴ http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf

⁵ http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF

⁶ http://www.eata.ee/wp-content/uploads/2009/11/Estonian_Cyber_Security_Strategy.pdf

⁷ <http://www.ssi.gouv.fr/IMG/pdf/2011-02->

⁸ [15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf](http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf)

⁸

http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber_eng.pdf;jsessionid=365A25B8FF75170FF9566570016DDEA9.1_cid165?__blob=publicationFile

⁹ <http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011>

¹⁰ <http://www.cybersecuritymarket.com/wp-content/uploads/2009/06/css0906.pdf>

¹¹ http://www.mit.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf

¹² <http://www.pmg.org.za/files/docs/100219cybersecurity.pdf>

¹³ Strategies such as the *International Strategy for Cyberspace* of the White House/USA (2011) has a broader scope than cyber security or cybercrime but these are listed as important “policy priorities”.

http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

See also USA – Department of Defence (2011): Strategy for Operating in Cyberspace

<http://www.defense.gov/news/d20110714cyber.pdf>

Cybersecurity strategies are setting policy goals, measures and institutional responsibilities in a fairly succinct manner. Generally, the primary concern is to ensure the confidentiality, integrity and availability (c-i-a) of computer data and systems and to protect against or prevent intentional and non-intentional incidents and attacks. Priority is given to critical information infrastructure protection (CIIP).

Some of these strategies contain also measures against cybercrime. Indeed, measures against cybercrime provide a criminal justice response to c-i-a attacks against computers and thus complement technical and procedural cybersecurity responses.

However, cybercrime comprises also offences committed by means of computer data and systems, ranging from the sexual exploitation of children to fraud, hate speech, intellectual property rights (IPR) infringements and many other offences. These are not necessarily part of cybersecurity strategies.

Furthermore, any crime may involve electronic evidence in one way or the other. While this may not be labelled "cybercrime", a cybercrime strategy would nevertheless need to ensure that the forensic capabilities be created that are necessary to analyse electronic evidence in relation to any crime, or that all law enforcement officers, prosecutors and judges are provided at least with basic skills in this respect.

Strategies and measures against cybercrime ("cybercrime control") thus follow a criminal justice rationale. They are linked to broader crime prevention and criminal justice policies and they are (or should be) aimed at contributing to the rule of law and the promotion of human rights.

In short, while strategies on cybersecurity and cybercrime control are interrelated, intersecting and complementary, they are not identical. A cybersecurity strategy does not address the full range of cybercrime issues, and a cybercrime strategy not the full range of cybersecurity issues.

Governments may therefore want to consider the preparation of specific cybercrime strategies that complement, add to or become components of cybersecurity strategies or policies.

The purpose of the present paper is to add impetus to such considerations. Following discussions at the Internet Governance Forum (Workshop 115 on Cybercrime Strategies) in Kenya, Nairobi, on 28 September 2011¹⁴, and the Council of Europe's Octopus conference (Strasbourg, France, 22 November 2011),¹⁵ this paper may eventually lead to a guidance document on cybercrime policies and strategies.

¹⁴ <http://www.intgovforum.org/cms/component/chronocontact/?chronoforumname=Workshops2011View&wspid=115>

¹⁵ www.coe.int/octopus

2 Cybercrime and cybersecurity: current concepts and strategies

2.1 Cybersecurity

A cursory review of cybersecurity strategies adopted or in preparation¹⁶ suggests that these are high-level policy documents motivated by the:

- reliance of society on cyber space which means that the security and resilience of and trust and confidence in ICT is a matter of national interest
- economic role and potential of ICT and the intention of maximising benefits and exploiting opportunities that these offer
- fact that cyber attacks – in particular against critical information infrastructure – may threaten national security. Thus, cybersecurity strategies are typically linked to national security and defence strategies.

Concepts, aims or definitions of “cybersecurity”, therefore, combine political (national interest and security) and technical dimensions whereby cybersecurity is typically defined as the protection of the confidentiality, integrity and availability of computer data and systems in order to enhance security, resilience, reliability and trust in ICT.

Some cybersecurity strategies, in their vision, refer to the need for the protection and promotion of human rights and the rule of law.¹⁷ However, the security, stability or resilience of the Internet so that people can exercise their freedom of expression and other rights seems not to be a primary objective of cybersecurity.¹⁸

Cybersecurity strategies appear to give highest priority to the protection of public and private sector critical information infrastructure as well as of government computer systems against:

- non-intentional incidents caused by malfunctioning of technology, coincidental failures, human failure, natural disasters and others
- intentional attacks by state and non-state actors, including botnet attacks to disrupt information infrastructure, unauthorised access and interception of data

¹⁶ See in the appendix the overview of cyber security strategies in Australia, Canada, Czech Republic, Estonia, France, Germany, India, Netherlands, South Africa, United Kingdom as examples.

For additional analyses or relevant texts on cyber- or information security see:

– ENISA (2010): Country reports – Overview http://www.enisa.europa.eu/act/sr/files/country-reports/enisa_country_reports_introduction.pdf

– OECD (2002): Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Paris <http://www.oecd.org/dataoecd/16/22/15582260.pdf>

¹⁷ The need to ensure that the “security of information systems and networks should be compatible with essential values of a democratic society” was already underlined in the OECD principles of 2002. The draft “European principles and guidelines for Internet resilience and stability” state that these principles should be guided by core European values, in particular human rights.

http://ec.europa.eu/information_society/policy/nis/docs/principles_ciip/quidelines_internet_fin.pdf

See also the US International Strategy for Cyberspace of 2011

http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

¹⁸ At the same time, the Council of Europe underlines that critical internet resources and the “universality, integrity and openness” of the Internet are to be protected so that everyone can benefit from human rights and fundamental freedoms (see Recommendation on the protection and promotion of Internet’s universality, integrity and openness

[https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Rec\(2011\)8&Language=lanEnglish&Ver=original&Site=COE&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383](https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Rec(2011)8&Language=lanEnglish&Ver=original&Site=COE&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383)

and communications (including computer espionage) or the manipulation or destruction of data and systems (including computer sabotage).¹⁹

Intentional attacks seem to be the primary concern. Threat actors listed are states, terrorists or criminals, whereby attribution and the blurring distinction between state and non-state actors are considered problems.

Cybersecurity strategies tend to focus on technical, procedural and institutional measures, such as risk and vulnerability analyses, early warning and response, incident management, information sharing, setting up of Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs), increased international cooperation and other measures to ensure protection, mitigation and recovery.

Criminal justice or other measures against cybercrime are usually not among the priorities of cybersecurity strategies. Some make none or only general reference to cybercrime, or specifically exclude cybercrime from the scope of the strategy. Others may include specific measures against cybercrime among many others.

The cybersecurity strategy of the United Kingdom (2009) is an exceptional case in that it refers specifically to a complementary cybercrime strategy (adopted in 2010).

Considering the political and technical dimensions of cybersecurity strategies, responsibility for coordinating, managing and implementing typically lays with national cybersecurity "boards", "councils" or "committees" composed of representatives of relevant institutions, including cabinet offices, national defence, intelligence, ministries of interior and others. The technical dimension is covered by institutions such as departments for ICT, information security agencies, as well as CERTs, CSIRTs of similar incident response institutions. Technical institutions seem to play a leading role in the development of cybersecurity strategies. Criminal justice authorities (with exceptions) seem to have only a subordinated role.

2.2 Cybercrime

Cybercrime may be defined in a narrow sense as any offence targeting computer data and systems or in a very broad sense as any offence involving a computer system. The first one risks being too restrictive as it would exclude phenomena that do exist in the physical world but have gained a different quality and impact through the use of computers, such as child pornography, fraud or intellectual property right violations. The latter would be too broad as most crime nowadays involves a computer in one way or the other.

It is therefore expedient to apply a definition that covers new types of crime as well as old types of crime using computers without being too broad and therefore meaningless. The definition should be sufficiently robust to cover all relevant types of conduct even if technology evolves and phenomena of cybercrime appear to change almost every day. Finally, it should be possible to operationalise it for criminal law purposes in order to meet the rule of law principle that there cannot be a crime without a law. Only conduct established as a criminal offence can be considered a crime.

¹⁹ This type of conduct is broadly covered by articles 2 to 6 of the Budapest Convention on Cybercrime, that is, illegal access, illegal interception, data and systems interference, and misuse of devices.

A definition should furthermore be widely accepted and not be limited to a specific country and the corresponding domestic legislation.

A concept or "definition" meeting these requirements, that is neither too narrow nor too broad, that is normative and that is widely accepted, is available with the Council of Europe's Budapest Convention on Cybercrime.²⁰ Under this treaty, cybercrime denotes:

- Offences against the confidentiality, integrity and availability of computer data and systems, that is, offences against computer data and systems, including illegal access, illegal interception, data and system interference, misuse of devices²¹
- Offences committed by means of computer systems. This list is limited²² to those "old" forms of crime that obtain a new quality through the use of computers, that is, computer-related forgery and fraud, child pornography and offences related to infringements of copyright and related rights on a commercial scale.²³

This concept is capable of capturing cases that consist of a combination of different types of conduct.²⁴

Although the Budapest Convention was prepared by the Council of Europe (with currently 47 European member states), Canada, Japan, South Africa and the USA participated in its elaboration and signed it. The USA ratified it and became a full party in 2006. Other non-European countries are in the process of accession to the Convention on Cybercrime (Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines and Senegal). The concept or "definition" of cybercrime as proposed by the Budapest Convention is widely shared and applied in practice.

In addition to offences against and by means of computer data and systems, the Budapest Convention addresses a further issue, namely, the question of electronic evidence in relation to any crime involving a computer system.²⁵ Obviously, even the broadest definition would not consider an offence where computers play an ancillary role²⁶ to constitute cybercrime.

However, governments – possibly as part of a cybercrime strategy – would have to address the challenge of creating the criminal justice capabilities necessary for the collection, analysis and use of electronic evidence not only in relation to crimes against and by means of computers²⁷ but in relation to any crime. This broadens the scope: since any offence may involve electronic evidence, not only a few specialised officers need to be trained, but more or less all law enforcement officers, prosecutors and judges.

²⁰ www.coe.int/cybercrime

²¹ The misuse of devices (article 6) which refers to the production, sale, procurement or otherwise making available of devices or data for the purpose of committing the above offences, such as "hacking" tools

²² However, the Budapest Convention contains a set of procedural law and international cooperation measures. These apply to any crime involving electronic evidence or committed by means of a computer system. This provides it with a very wide scope (see article 14).

²³ An additional Protocol covers the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189).

²⁴ For example, fraud cases where Trojans are used to steal banking information and intercept online transactions may comprise illegal access, illegal interception, data and systems interference, as well as forgery and fraud. See the case documented by M 86 Security (White Paper): Cybercriminals Target Online Banking Customers (August 2010).

http://www.m86security.com/documents/pdfs/security_labs/cybercriminals_target_online_banking.pdf.

²⁵ See Article 14 of the Budapest Convention on the scope of procedural provisions.

²⁶ Such an email communication in a case of kidnapping.

²⁷ Which include mobile and smart phones and similar devices.

As indicated above, measures against cybercrime are often referred to in cybersecurity strategies²⁸ and include, for example, the strengthening of:

- legislation, including global harmonisation
- operational law enforcement capacities through additional resources and powers
- law enforcement and judicial training
- interagency cooperation
- industry/law enforcement cooperation
- international cooperation.

It seems that the United Kingdom is one of a few countries²⁹ that complemented its cybersecurity strategy with a specific strategy on cybercrime.³⁰

The "Cyber Crime Strategy" – presented to the UK Parliament by the Home Office in March 2010 – builds on the UK Cyber Security Strategy of 2009, but focuses more specifically on new offences committed by using new technology, that is, offences against computer data and systems, and old offences committed using new technology, including fraud and financial crime, threats to children, hate crimes, harassment and political extremism. Cybercrime is considered international crime and "the compatibility of criminal offences and investigative measures across a range of jurisdictions is as one of the most effective ways of enabling international cooperation".³¹

The vision of the Cyber Crime Strategy is identical with that of the Cyber Security Strategy, namely that "citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space: working together, at home and overseas, to understand and address the risks, to reduce the benefits to criminals and terrorists, and to seize opportunities in cyber space to enhance the UK's overall security and resilience."³²

Measures to be undertaken by the Home Office against cybercrime include:

- Coordinate activity against cybercrime across Government, including clear ownership for measures against cybercrime, review of legislation, establishing standards and promoting duty of care
- Reduce direct harms by making the internet a hostile environment for financial criminals and child abuse predators, including effective law enforcement and criminal justice response through specialised units and intelligence sharing, developing better understanding of scale and scope of cyber crime through reporting systems for public and business, producing a regular strategic overview of the threat to children and young people, developing tools, tactics and technology with industry to ensure that law enforcement are able to investigate online criminals
- Raise public confidence in the safety and security of the internet, not only through tackling crime and abuse, but through the provision of accurate and easy-to-understand information to the public on threats

²⁸ Such as those of Australia, Canada, France, Germany, India (draft) or Netherlands.

²⁹ Another example is New Zealand Police(2007): E-crime Strategy to 2010

<http://www.police.govt.nz/resources/2007/e-crime-strategy/e-crime-strategy.pdf>

³⁰ <http://www.official-documents.gov.uk/document/cm78/7842/7842.pdf>

³¹ Page 10.

³² Page 17.

- Support industry leadership to tackle cyber crime and work with industry to make products and services safer
- Work with international partners to tackle the problem collectively.

While cybersecurity strategies address the issue of cybercrime only to some extent and while only few countries adopted specific cybercrime strategies, a wide range of measures has been taken by governments, institutions, the private sector or international organisations that could form part of cybercrime strategies.

These range from reporting and intelligence systems, specific legislation, high-tech crime or other specialised units and forensic capabilities, to law enforcement and judicial training, law enforcement/service provider and other types of public-private cooperation, and international cooperation. Special attention has been given to the protection of children, in particular against sexual exploitation, and is increasingly being given to financial investigations.

Strategies or measures against cybercrime follow a criminal justice logic and should therefore be embedded in rule of law and human rights principles.

Article 15 of the Budapest Convention helps find a balance between an obligation of the state to protect people against crime on the one hand, and the need to limit law enforcement powers on the other hand. It establishes a number of general principles with regard to conditions and safeguards and makes reference to international human rights standards.

General rule of law principles include:

- There shall be no punishment without a law³³
- Everyone has the right to a fair trial, including the presumption of innocence³⁴
- Any interference in the rights of individual can only be in accordance with the law and as is necessary in the public interest – including crime prevention – or the protection of the rights of others.³⁵ This means that investigative measures – in particular if they entail an intrusion into rights – must be prescribed by law
- Anyone whose rights are violated must have the right to an effective remedy³⁶
- States need to put in place a framework that allows to reconcile different interests that are to be protected
- States have a positive obligation to protect the rights of individuals, according to the case law of the European Court of Human Rights. This may include criminal law and effective enforcement to bring offenders to justice.³⁷

³³ See Article 7 of the European Convention of Human Rights or Article 15 of the International Covenant on Civil and Political Rights.

³⁴ See Article 6 of the European Convention on Human Rights or Article 14 of the International Covenant on Civil and Political Rights

³⁵ See for example Article 8 of the European Convention of Human rights:

"1 Everyone has the right to respect for his private and family life, his home and his correspondence.
2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

³⁶ See Article 13 of the European Convention of Human Rights

³⁷ See for example, K.U. v. Finland

In addition to these general ones, a number of principles apply to the procedural powers of law enforcement:

- Principle of proportionality, meaning in particular that “the power or procedure shall be proportional to the nature and circumstances of the offence”.³⁸ For example, particularly intrusive measures, such as interception, are to be limited to serious offences
- Judicial or other independent supervision
- Grounds justifying the application of the power or procedure and the limitation on the scope or the duration
- Powers and procedures must be reasonable and “consider the impact on the rights, responsibilities and legitimate interests of third parties”.³⁹

If these principles are respected, an appropriate balance can be found with regard to criminal justice measures against cybercrime.

In practice, the balance is the result of a discursive process. In many countries, legislation and the practice of cybercrime enforcement are subject to controversial debates in media and parliaments or challenged before (constitutional) courts. This is a reflection of functioning checks and balances in a democratic state governed by the rule of law.

For that reason, Article 15 refers the modalities and implementation or the specific conditions for specific investigative measures in a specific country or situation to the domestic legal and judicial system.

With regard to cybersecurity, however, such a balance appears to be more difficult to find. To the extent that cybersecurity is regarded as an issue of national interest, the risk is that cybersecurity is removed from the criminal justice arena – with its rule of law and human rights safeguards – to the national security arena with its exceptions to rule of law and human rights guarantees.

³⁸ See paragraph 146 of the Explanatory Report

³⁹ Article 15 (3) Budapest Convention

3 Cybercrime policies and strategies: possible elements

The approach to cybercrime in a specific country is influenced by many factors, including the nature of the threat, the state of the criminal justice system, the level of respect for human rights and the rule of law (including the approach to privacy, data protection and freedom of expression), the cybersecurity landscape or the relationship between public and private sectors.⁴⁰

A blue-print or “model” cybercrime strategy may therefore be of limited value. However, the following could be elements of cybercrime strategies and could be further elaborated and adapted to the specific conditions of a country.

3.1 Scope of a cybercrime strategy

Cybercrime may be understood to comprise

- offences against the confidentiality, integrity and availability of computer data and systems (as a minimum illegal access, illegal interception, data and system interference (including denial of service attacks and other botnet and malware activity) as well as the misuse of devices for the commission of such offences⁴¹
- offences committed by means of computer data and systems, specifically those that have acquired a different quality or scope through the use of computers, including as minimum child pornography or the sexual exploitation and abuse of children, forgery and fraud, and offences related to intellectual property right infringements.⁴²

In addition to offences against and by means of computers, electronic evidence can play a role with regard to almost any offence. Even if an ancillary role of computers does not constitute cybercrime, a cybercrime strategy may need to address the question of admissibility of electronic evidence in criminal proceedings and ensure that law enforcement and other criminal justice authorities are capable of collecting, analysing and presenting electronic evidence.

While offences against computer data and systems gain in impact, in particular when critical information infrastructure is attacked, it is in particular offences committed by means of computers that cause very large damage to individuals and public and private sector organisations. The need to address the question of electronic evidence implies that the vast majority of law enforcement officers, prosecutors and judges of a country would need to be trained.

The scope, damage and impact of cybercrime and the wide range of measures to be taken suggest that there is justification for a strategic approach and the allocation of resources to address cybercrime and electronic evidence.

⁴⁰ Comment made by Monika Josi, Roger Halbheer and Jean-Christophe Le Toquin

⁴¹ These correspond to articles 2 to 6 of the Budapest Convention on Cybercrime.

⁴² These correspond to articles 7 to 10 of the Budapest Convention on Cybercrime. Article 9 is about “child pornography” while the broader concept of the sexual exploitation and abuse of children is subject of the Lanzarote convention CETS 201 (Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse).

3.2 Objective of a cybercrime strategy

Overall objective: to ensure that the rule of law applies and that legitimate rights are protected also in the ICT and online environment

Specific objective: to ensure an effective criminal justice response to offences against the confidentiality, integrity and availability of computers and by means of computers as well as to any offence involving electronic evidence.

3.3 Measures

3.3.1 Cybercrime reporting and intelligence

Reporting channels should be established to allow users but also public and private sector organisations report cybercrime. This will enhance the understanding of scope, threats and trends and the collation of data to detect patterns of organised criminality.⁴³

Given the fast evolution of technologies and with it cybercrime and techniques used by criminals, building intelligence is of particular importance to assess threats and predict trends, and thus to help adjust measures against strategies.

3.3.2 Prevention

Public education and awareness, the empowerment of users and technical and other measures should be essential elements of cybercrime strategies. Specific measures should be envisaged for the online protection children⁴⁴ and for fraud prevention.⁴⁵

3.3.3 Legislation

States should adopt legislation that is harmonised with international standards⁴⁶ in order to:

- criminalise conduct⁴⁷
- provide law enforcement with procedural law tools for efficient investigations
- establish safeguards and conditions limiting investigative powers⁴⁸ as well as adopting data protection regulations.⁴⁹

⁴³ Examples are the Internet Complaint Center (http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf). The "Melde- und Analysestelle Informationssicherung" (MELANI) in Switzerland (<http://www.melani.admin.ch>), the National Fraud Reporting Centre in the UK (<http://www.actionfraud.org.uk/home>), or Signal Spam in France (<https://www.signal-spam.fr/>).

⁴⁴ http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Protecting%20children/Default_en.asp

⁴⁵ For examples of different types of fraud prevention measures see: <http://www.ic3.gov/preventiontips.aspx>
http://www.stoppbetrug.ch/4/fr/1prevention_methodes_descroquerie/40201ventes_aux_encheres.php
<http://www.polizei-nrw.de/koeln/Vorbeugung/kriminalitaet/INTERNET-und-datenkriminalitaet/>
<http://www.visa.ca/en/merchant/fraud-prevention/index.jsp>

⁴⁶ Budapest Convention on Cybercrime www.coe.int/cybercrime

⁴⁷ For example, articles 2 to 10 of the Budapest Convention as a minimum

⁴⁸ See article 15 of the Budapest Convention on Cybercrime

⁴⁹ For example in line with the Data Protection Convention 108 of the Council of Europe <http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&DF=22/08/2011&CL=ENG>

3.3.4 High-tech crime and other specialised units

Specialised units, such as high-tech crime units, prosecution services responsible for cybercrime and services for cyberforensics will need to be created.⁵⁰

3.3.5 Interagency cooperation

Cybercrime is not the sole responsibility of a specific (specialised) unit. For example, high-tech crime units may provide support to other services investigating fraud, money laundering or child pornography, or cooperate with CERTS or other institutions responsible for cybersecurity. Specific procedures and mechanisms for interagency cooperation would need to be established

3.3.6 Law enforcement training

The objective of a specific law enforcement training strategy could be to ensure that law enforcement officers have the skills/competencies necessary for their respective functions to

- investigate cybercrime
- secure electronic evidence
- and carry out computer forensics analyses for criminal proceedings
- assist other agencies
- contribute to network security.

The first step towards such a training strategy would be a training needs analysis (covering requirements from first responders to generic investigators, specialist investigators, internet crime investigators, covert internet crime investigators, network crime investigators, digital forensic investigators and managers).⁵¹

3.3.7 Judicial training

A judicial training concept should ensure that all judges and prosecutors have at least basic knowledge to deal with cybercrime and electronic evidence. This means that such training needs to be integrated into the regular judicial training system of a country. A coherent concept would be required to ensure this.⁵² The objectives could be:

- to enable training institutes to deliver initial and in-service cybercrime training based on international standards
- to equip the largest possible number of future and practicing judges and prosecutors with basic knowledge on cybercrime and electronic evidence
- to provide advanced training to a critical number of judges and prosecutors
- to support the continued specialisation and technical training of judges and prosecutors

⁵⁰ The Council of Europe under its CyberCrime@IPA joint project with the European Union and in cooperation with the EU Cybercrime Task Force is preparing a good practice study on "specialised cybercrime units". This study is to be available by the time of the Octopus conference (21-23 November 2011). See www.coe.int/cybercrime

⁵¹ The Council of Europe – under its CyberCrime@IPA joint project with the European – is supporting countries of South-eastern Europe in the development of such strategies.

⁵² The Council of Europe – under its Global Project on Cybercrime – developed such concept in 2009. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/default_en.asp

- to contribute to enhanced knowledge through networking among judges and prosecutors
- to facilitate access to different training initiatives and networks.

3.3.8 Public/private (LEA/ISP) cooperation

All cybersecurity strategies underline the need for public/private cooperation. With respect to cybercrime, cooperation between law enforcement and service providers is particularly essential. Memoranda of Understanding or other types of agreements could be considered to provide a framework for efficient cooperation that defines expectations, responsibilities, authorities but also limitations and that ensures that the rights of users are protected.⁵³

Positive examples of public/private cooperation are available⁵⁴ and could be built upon.

3.3.9 Effective international cooperation

Cybercrime is transnational crime involving multiple jurisdictions. Efficient international police to police and judicial cooperation is required to preserve volatile electronic evidence. This includes direct cooperation between high-tech crime units and between prosecutors of different countries. 24/7 points of contact in line with Article 35 of Budapest Convention and as promoted by the G8 High-tech Crime Sub-group should be established.

Chapter III of the Convention on Cybercrime provides a legal framework for international cooperation with general and specific measures, including the obligation of countries to cooperate to the widest extent possible, urgent measures to preserve data and efficient mutual legal assistance. States should also consider accession to this treaty to make use of these provisions.

3.3.10 Financial investigations and prevention of fraud and money laundering

Obtaining financial or other economic benefits has been one motivation of cybercriminals from the very beginning. However, there is general agreement that generating proceeds is now the primary purpose of cybercrime. The type of cybercrime in this respect is fraud.⁵⁵

Public authorities but also private sector organisations should pay particular attention to the prevention of fraud and money laundering but also to financial investigations to search, seize and confiscate proceeds from cybercrime. Such measures may include cybercrime reporting systems; prevention and public awareness; regulation licensing and supervision; risk management and due diligence, harmonisation of legislation, interagency cooperation, public/private cooperation and information exchange⁵⁶ and other measures.

⁵³ In 2008, the Council of Europe's Octopus Conference adopted guidelines that can help structure such cooperation.

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp

⁵⁴ Examples include cooperation with CERTS, Signal Spam in France (<https://www.signal-spam.fr/>) and others.

⁵⁵ For an A-Z of fraud schemes see http://www.actionfraud.org.uk/a-z_of_fraud

⁵⁶ Information Sharing and Analysis Centres (ISAC) for the financial sector <http://www.fsisac.com/>, <http://www.samentagencybercrime.nl/>, http://www.samentagencybercrime.nl/Informatie_knooppunt/Sectorale_ISACs/FIISAC?p=content

3.3.11 Protection of children

Empowering children and fostering their trust and confidence in the Internet together with the protection of their dignity, security and privacy requires a comprehensive set of measures that go beyond the scope of cybercrime or cybersecurity strategies.⁵⁷ However, special attention is to be paid to the prevention and control of the sexual exploitation and abuse of children. The Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse provides a framework for a comprehensive set of measures.⁵⁸

Countries need criminalise child pornography and other conduct in line with international standards⁵⁹ and establish the conditions for effective enforcement.

3.4 Responsibilities for management, coordination, implementation, monitoring

If cybercrime policies or strategies are adopted, responsibilities for implementation need to be assigned and the strategy is to be managed, coordinated and monitored. Public institutions responsible for rule of law matters would need to take the lead while at the same time multi-stakeholder involvement is to be ensured.

3.5 Technical assistance for capacity building⁶⁰

Many countries may need technical assistance in order to create the capacities necessary for the implementation of legislation, the creation of specialised units, training and other measures foreseen under a cybercrime strategy.

A coherent strategy on cybercrime would certainly help mobilise technical assistance and allow public and private sector donors to understand and decide to what they are contributing.⁶¹

In short, the adoption of a cybercrime strategy may serve facilitate technical assistance.

57

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Protecting%20children/Default_en.asp

⁵⁸ <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=1&DF=&CL=ENG>

⁵⁹ See Article 9 of the Budapest Convention and the Lanzarote Convention

⁶⁰ The question of capacity building was addressed in Workshop 23 at the IGF 2010 (Lithuania)

<http://www.intgovforum.org/cms/component/chronocontact/?chronoforname=WSProposalsReports2010View&wspid=23>

The need for a global capacity building effort was furthermore underlined by the Octopus conference 2010

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/2079_IF10_messages_1p%20key%20prov%2026%20mar%2010.pdf

The United Nations Crime Congress 2010 (Salvador, Brazil) also showed that there was broad agreement on the need for capacity building against cybercrime

http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf

⁶¹ Examples of specific projects include those of the Council of Europe, including joint projects with the European Union (www.coe.int/cybercrime). The Commonwealth is currently preparing a Cybercrime Initiative (<http://www.commonwealthigf.org/blog/the-commonwealth-cybercrime-initiative/>)

4 Cybercrime and cybersecurity strategies: complementarity

At this point, one may conclude that cybersecurity and cybercrime control are different but inter-related and intersecting concepts (at least in the way they are understood and applied so far). Cybersecurity and cybercrime control measures complement each other.

The primary interest of cybersecurity strategies is to ensure the confidentiality, integrity and availability (“c-i-a”) of ICT (in particular critical information infrastructure) and the services built on it. They are covering non-intentional ICT security incidents and, more importantly, intentional attacks by state and non-state actor, including criminals and terrorists. In terms of measures, the focus is on technical, administrative and procedural measures to protect systems, in particular critical information infrastructure, to increase their resilience, to prevent, detect and manage incidents, to ensure coordinated responses to incidents and recovery, as well as building confidence and trust in ICT and the digital economy, and finally on national security and defence. Given the reliance of societies on ICT, cybersecurity strategies are contributing to larger political, security, economic and social interests of countries. Cybersecurity strategies are thus interdisciplinary and comprise multiple stakeholders.⁶²

The primary interest of cybercrime strategies is crime prevention and criminal justice that is to ensure that the rule of law applies also in the ICT and borderless online environment. Like cybersecurity strategies they cover attacks against the confidentiality, integrity and availability against ICT by state and non-state actors. However, cybercrime strategies – while also covering preventive and not excluding technical measures – would focus primarily on the investigation, prosecution and adjudication of offenders. This means that cybercrime strategies and measures put emphasis on rule of law and human rights principles, including safeguards and conditions regarding investigative and other procedural measures. It is indicative that public authorities responsible for the rule of law (ministries of justice and interior, prosecution services, law enforcement agencies) have primary responsibility for cybercrime matters but play only a secondary role in cybersecurity strategies.

Cybercrime control goes beyond attacks against ICT and addresses offences also by means of ICT. This is particularly true for offences that have acquired a new scope and quality in cyberspace such as the sexual exploitation of children, fraud, the terrorist use of the Internet, infringements of intellectual property rights and other offences. Offences by means of ICT would normally not be covered by cybersecurity strategies.

Moreover, cybercrime strategies may need to address the fact that any offence may involve electronic evidence which entails a large-scale effort to enhance criminal justice capabilities.⁶³

Nevertheless, cybersecurity and cybercrime strategies complement and reinforce each other cross-wise and at different levels.

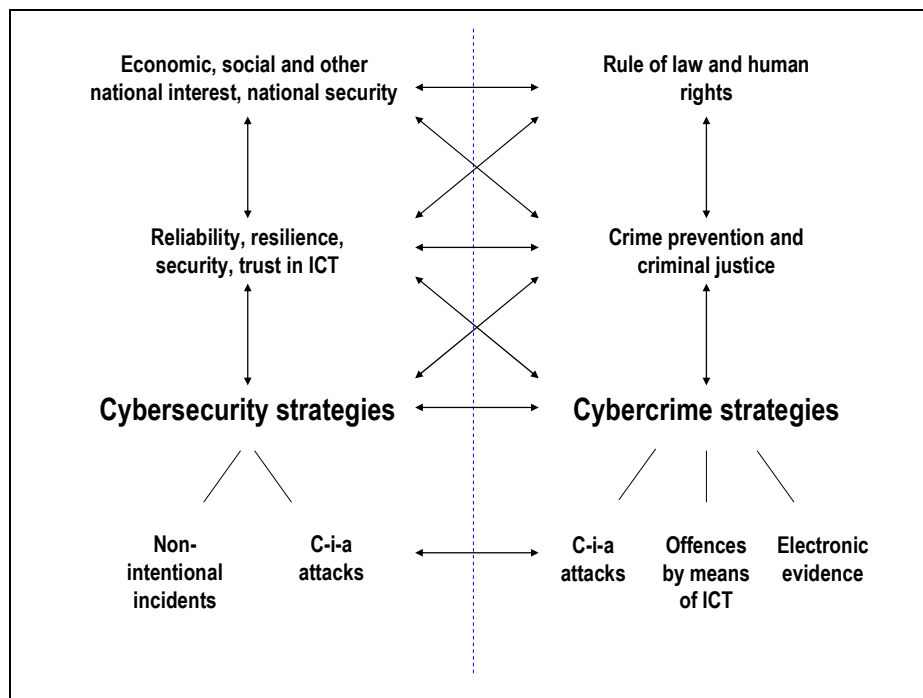
The complementarity is obvious with respect to the response to c-i-a attacks: While cybersecurity covers a wide range of technical and procedural measures to respond to

⁶² Comment made by Markko Künnapu.

⁶³ In this sense, cybercrime strategies would need address a challenge that is not even considered cybercrime.

intentional attacks against ICT and to ensure the confidentiality, integrity and availability of ICT (ranging from prevention to protection and recovery), cybercrime strategies focus on the criminal justice response to c-i-a attacks.

Or to develop Vinton Cerf's metaphor further, if a cybersecurity strategy is about "fire brigades" ('When a house is on fire, the priority is to put down the fire to mitigate the damage, to repair the house and make it functioning again. Cybersecurity is about efficient fire brigades')⁶⁴, then a cybercrime strategy is about criminal justice: if somebody puts one house after the other on fire it is necessary and effective to investigate and prosecute the offender and put him or her behind bars to prevent further damage.



However, this complementary goes further than that. It is also obvious with regard to higher level objectives of cybercrime and cybersecurity strategies. For example, increased reliability, resilience, security and trust in ICT contribute to crime prevention and criminal justice and vice versa, but these also contribute to the rule of law and human rights (including privacy and the freedom of expression). Or increased cybersecurity contributes to crime prevention and criminal justice and vice versa. And the rule of law and human rights serve (or should serve) national interests and security.

⁶⁴ During a workshop at the 2010 Internet Governance Forum in Vilnius, Lithuania, on international cooperation on cybersecurity. For the background paper see: http://www.afilias.info/webfm_send/135

5 Conclusion

As suggested earlier in this paper, cybersecurity and cybercrime control are related but nevertheless different concepts. The same applies to the respective strategies. They pursue different objectives and comprise different measures. A cybersecurity strategy does not address the full range of cybercrime, and a cybercrime strategy not the full range of cybersecurity issues. At the same time, they are intersecting and interrelated and complement each other.⁶⁵

All of this suggests two options to promote both cybersecurity as well as the prevention and control of cybercrime:

Option 1: Governments should develop specific cybercrime strategies in addition to those for cybersecurity. If this option is chosen, synergies and complementarity between otherwise separate strategies need to be built in; or

Option 2: Governments should enhance cybercrime components within cybersecurity strategies. However, this would require reconsidering and broadening the concept of cybersecurity to encompass criminal justice objectives and principles and to "take cybersecurity out of the national security corner".⁶⁶

With regard to both options, the following may be taken into account:

- A distinct approach to the prevention and control of cybercrime will help identify the measures to be taken, establish responsibilities for such measures and ensure that criminal justice considerations are fully taken into account. These include rule of law and human rights principles.
- It would seem that when cybersecurity and cybercrime are dealt with by entities specialised in ICT, rule of law and criminal justice requirements tend to be neglected. Not everything that is technically feasible is also acceptable from a rule of law point of view. Rule of law authorities (such as ministries of justice or interior or prosecution services) should therefore take a leading role in cybercrime strategies.
- Cybersecurity – including the protection of critical information infrastructure – is increasingly considered an issue of national interest. This focus carries the risk that cybersecurity measures are removed from the criminal justice arena – with its rule of law and human rights safeguards – to the national security arena and its exceptions to rule of law and human rights guarantees. Separate cybercrime strategies or strong cybercrime components in cybersecurity strategies may help strengthen such guarantees.
- Cybercrime – understood as offences not only against but also by means of computer systems – causes major damage to societies. And most other types of crime involve electronic evidence in one way or the other. The cost of cybercrime and the issue of electronic evidence, therefore, justify major investments in cybercrime strategies.

⁶⁵ This section takes into account the discussions in "Workshop 115 – Cybercrime strategies" at the Internet Governance Forum in Nairobi, Kenya, 28 September 2011.

⁶⁶ Comment made by Roger Halbheer, Microsoft.

- The adoption of a cybercrime strategy may help mobilise technical assistance for capacity building.⁶⁷
- While criminal justice is a prerogative of criminal justice authorities and governments, it involves a multitude of other actors, including private sector entities. Multi-stakeholder approaches should therefore be pursued when designing, implementing and managing cybercrime strategies. This may help avoid over-regulation and encourage agreements below the level of formal regulation and, in particular, of criminal law.⁶⁸
- Attribution of an attack or intrusion to individual offenders, criminal or terrorist organisations or a foreign state remains a major problem. Treating an attack as cybercrime to start with may help de-escalate situations and prevent open conflicts.
- The confusion of the concepts of cybersecurity and cybercrime seems to have been hindering international agreement in recent years. A clarification of the concepts of cybersecurity versus cybercrime may thus facilitate progress in this respect: it would allow states to make use of existing international treaties on cybercrime – that is, the Budapest Convention – while engaging in negotiations on norms or codes of conduct for state behaviour that are primarily aimed at preventing conflicts between states in cyberspace.⁶⁹

⁶⁷ This point was made repeatedly at the Nairobi Internet Governance Forum: a number of African countries have adopted legislation on cybercrime but are not in a position to apply.

⁶⁸ These points were underlined at IGF workshop 115 by Bill Smith.
https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf

⁶⁹ Such norms of state behaviour and confidence building measures limited to the politico-military dimension are being discussed at the level of the Organisation for Security and Cooperation in Europe, OSCE. Some states proposed in September 2011 to negotiate a non-binding code of conduct within the United Nations. <http://blog.internetgovernance.org/pdf/UN-infosec-code.pdf>
The London Conference on Cyberspace (1-2 November 2011) is to discuss such principles as well.
<http://www.fco.gov.uk/en/global-issues/london-conference-cyberspace/>

6 Appendix: Examples of cybersecurity and cybercrime strategies

Country/ strategy	Vision/objectives/issues to be addressed	Institutional responsibility	Strategic priorities and measures	Measures on cybercrime
<p>Australia Cyber Security Strategy (2009)⁷⁰</p>	<ul style="list-style-type: none"> - High risk to Australian economy from malware and computer intrusion by state and non-state actors - Cyber security defined as: "Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means" - "The aim of the Australian Government's cyber security policy is the maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy" - The objectives of the cyber security policy are that: <ul style="list-style-type: none"> - "All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online - Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers - The Australian Government ensures its information and communications technologies are secure and resilient." 	<p>The strategy was prepared by the Attorney General's Department and represents the strategy of the Australian Government</p> <p>Two new organisations created:</p> <ul style="list-style-type: none"> - CERT Australia as the national coordination point within the Gov for security information and more effective international cooperation - Cyber Security Operations Centre to identify sophisticated attacks and facilitate operational responses 	<p>Strategic priorities are:</p> <ul style="list-style-type: none"> - Improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest - Educate and empower all Australians with the information, confidence and practical tools to protect themselves online - Partner with business to promote security and resilience in infrastructure, networks, products and services - Model best practice in the protection of government ICT systems - Promote a secure, resilient and trusted global electronic operating environment that supports Australia's national interests - Maintain an effective legal framework and enforcement capabilities to target and prosecute cybercrime - Promote the development of a skilled cyber security workforce with access to research and development to develop innovative solutions 	<p>Under the priority "legal and law enforcement" measures include:</p> <ul style="list-style-type: none"> - providing additional resources for security and law enforcement agencies to enhance operational capabilities - ensuring linkages and intelligence sharing between cyber security and law enforcement efforts - ensuring Australia's criminal and civil legal framework is robust and keeps pace with developments - providing Australian legal with the requisite level of technological knowledge and understanding to effectively administer these laws - promoting the harmonisation of Australia's legal framework for cyber security with other jurisdictions and internationally to facilitate information sharing and law enforcement cooperation across geographical borders.

⁷⁰ [http://www.ag.gov.au/www/aqd/rwpattach.nsf/VAP/\(4CA02151F94FFB778ADAEC2E6EA8653D\)~AG+Cyber+Security+Strategy+-+for+website.pdf/\\$file/AG+Cyber+Security+Strategy+-+for+website.pdf](http://www.ag.gov.au/www/aqd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf)

Country/ strategy	Vision/objectives/issues to be addressed	Institutional responsibility	Strategic priorities and measures	Measures on cybercrime
Canada Cyber Security Strategy (2010) ⁷¹	<ul style="list-style-type: none"> - Canada's economy relies heavily on the Internet - "Cyber attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information." - Main risks: <ul style="list-style-type: none"> - State sponsored cyber espionage and military activity - Terrorist use of the internet - Cybercrime by organised criminals - Threat is evolving - Three pillars to meet this challenge: <ul style="list-style-type: none"> - Securing Government systems - Partnering to secure vital cyber systems outside the federal Government - Helping Canadians to be secure online 	<ul style="list-style-type: none"> - Public Safety Canada will coordinate implementation of strategy - Other stakeholders: <ul style="list-style-type: none"> - Canadian Cyber Incident Response Centre (within Public Safety Canada) Communication Security Establishment Canada - Canadian Security Intelligence Service - Royal Canadian Mounted Police - Treasury Board Secretariat - Foreign Affairs and International Trade Canada - Department of National Defence and the Canadian Forces 	<ul style="list-style-type: none"> - Securing Government systems: <ul style="list-style-type: none"> - Establishing clear federal roles and responsibilities - Strengthening the security of federal cyber systems - Enhancing cyber security awareness throughout Government - Partnering to secure vital cyber systems outside the federal Government <ul style="list-style-type: none"> - Partnering with the Provinces and Territories - Partnering with the private sector and critical infrastructure sectors - Helping Canadians to be secure online <ul style="list-style-type: none"> - Combating cybercrime - Protecting Canadians online 	<p>Combating cybercrime is one component under the pillar "helping Canadians to be secure online"</p> <p>Measures include:</p> <ul style="list-style-type: none"> - Equipping police to protect against identity theft and transnational cybercrime with legislative authorities and financial resources - Establishment of a centralised Integrated Cyber Crime Fusion Centre to respond to cyber attacks against Government or critical infrastructure - Further legislative reforms on <ul style="list-style-type: none"> - Sexual exploitation of children - Requiring ISPs to maintain interception capabilities - Requiring ISPs to provide customer identification information - Increase cooperation with treaty partners in fighting serious crimes

⁷¹ <http://www.publicsafety.gc.ca/prq/ns/cbr/fl/ccss-scc-eng.pdf>

Country/ strategy	Vision/objectives/issues to be addressed	Institutional responsibility	Strategic priorities and measures	Measures on cybercrime
<p>Czech Republic Cyber Security Strategy for the Czech Republic for the 2011 – 2015 Period⁷²</p>	<ul style="list-style-type: none"> – ICTs have a major effect on the functioning of advanced societies and economies – ICTs and ICT-dependent societies are vulnerable <p>“The Strategy represents an institutional framework, which constitutes a part of the Czech Republic’s security system. The framework document marks the beginning of an active national cyber defense policy.”</p> <p>Cyber security “needed to build up a credible information society with solid legal foundations, which is committed to a secure cyber transmission and processing of information in all domains of human activities and makes sure that the information can be used and shared freely and safely.”</p> <p>Objectives include</p> <ul style="list-style-type: none"> – “protection against threats which information and communication systems and technologies (hereinafter “ICTs”) are exposed to, and mitigation of potential consequences in the event of an attack against ICTs.” – “to maintain a safe, secure, resistant and credible environment that makes use of available opportunities offered by the digital age. The strategy focuses mainly on unimpeded access to services, data integrity and confidentiality of the Czech Republic’s cyberspace and is coordinated with other related strategies and concepts.” 	<p>The implementation, operation and security of credible information and communication systems is a duty of the Czech Republic and a responsibility of all levels of government and administration, the private sector and the general public</p>	<ul style="list-style-type: none"> – Legislative framework – Strengthening of cyber security of public administration and of ICT of critical infrastructure – Establishment of national CERT – International cooperation – Cooperation of the State, private sector and academia – Increased cyber security awareness <ul style="list-style-type: none"> – Adequacy of measures: risk analysis and international standards to protect and guarantee national cyber security and respect privacy, respect privacy, fundamental rights and liberties, free access to information and other democratic principles. The Czech Republic will focus on their adequacy, balancing the need to guarantee security against respect for fundamental rights and liberties. 	<p>Under legislative framework:</p> <p>“The Czech Republic will improve legislative and procedural steps so that the cyber security field ultimately comprises prevention, detection, reaction and measures designed to identify and combat cyber crime.”</p>

Country/ strategy	Vision/objectives/issues to be addressed	Institutional responsibility	Strategic priorities and measures	Measures on cybercrime
<p>Estonia Cyber Security Strategy (2008)⁷³</p>	<p>Cyber attacks against advanced information societies aimed at undermining the functioning of public and private sector information systems pose a threat to international security. Coordinated large-scale attacks against Estonia of 2007 and recurrence of incidents beginning of a new era where the security of cyberspace acquires a global dimension and protection of critical information systems becomes a matter of national security</p> <p>Cyber security is about “reducing the vulnerability of cyberspace, preventing cyber attacks in the first instance and, in the event of an attack, ensuring a swift recovery of the functioning of information systems”.</p> <p>Cyber Security Strategy linked to national security and defence policies but also to Estonian Information Society Strategy 2013 of 2007.</p>	<ul style="list-style-type: none"> – Strategy prepared by the “Cyber Security Strategy Committee” led by the Ministry of Defence with Ministries of Education and Research, of Justice, of Economic Affairs and Communication, of Internal Affairs and of Foreign Affairs – The Committee, in cooperation with the private sector responsible for developing implementation plans – Cyber Security Council to monitor implementation 	<ul style="list-style-type: none"> – The development and large-scale implementation of a system of security measures <ul style="list-style-type: none"> - Protection of critical information infrastructure - Development and Implementation of a System of Security Measures - Strengthening of Organisational Co-operation, including setting up of Cyber Security Council – Increasing competence in cyber security <ul style="list-style-type: none"> - Organisation of training in cyber security - Enhancing research and development – Improvement of the legal framework for supporting cyber security – Development of international co-operation <ul style="list-style-type: none"> - Promoting cyber security and defence globally - Promote Budapest Convention on Cybercrime globally - Estonian expertise in international organisations - Participation in the work of international organisations – Raising awareness on cyber security 	<p>“The Cyber Security Strategy does not include national measures to target cyber crime; this is because the Ministry of Justice has already devised a criminal policy addressing the fight against cyber crime and also because the Ministry of Internal Affairs has prepared a draft of Estonia’s internal security priorities until 2015”</p> <p>However, the strategy comprises some international measures to:</p> <ul style="list-style-type: none"> – raise awareness of cybercrime and cyber security – develop international cooperation – promote the Budapest Convention on Cybercrime worldwide and to provide assistance to accession by countries

Country/ strategy	Vision/objectives/issues to be addressed	Institutional responsibility	Strategic priorities and measures	Measures on cybercrime
<p>France Défense et sécurité des systèmes d'information – Stratégie de la France⁷⁴</p>	<p>Cyber security is defined as the ability to ensure the confidentiality, integrity and availability of information systems against incidents emanating from cyber space:</p> <p>« état recherché pour un système d'information lui permettant de résister à des événements issus du cyberspace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles »</p> <p>The four objectives of the strategy are :</p> <ol style="list-style-type: none"> 1. To be a global power in the field of cyber defence 2. To guarantee the freedom of decision-making by public authorities of France by protecting information related to national sovereignty (ensuring confidentiality of communication) 3. To reinforce the cyber security of critical national infrastructure 4. To assure security in cyber space 	<p>Strategy prepared by the Agence Nationale de la Sécurité des Systems d'Information (ANSSI)</p>	<p>Seven axes of efforts :</p> <ol style="list-style-type: none"> 1. Anticipate and analyse 2. Detect, alert and react 3. Improve and make sustainable scientific, technical, industrial and human capacities 4. Protect information systems of the State and of operators of critical infrastructure 5. Adapt legislation 6. Develop international cooperation 7. Communicate to inform and convince 	<ul style="list-style-type: none"> – The fight against cybercrime is considered one of the bases of cyber security. – Objective 4 refers to improvement of legislation and international cooperation with respect to cybercrime – Axis 6 refers to international cooperation against cybercrime

Country/ strategy	Vision/objectives/issues to be addressed	Institutional responsibility	Strategic priorities and measures	Measures on cybercrime
<p>Germany Cyber Security Strategy for Germany (2011)⁷⁵</p>	<p>“Cyber security” defined as a situation “in which the risks of global cyberspace have been reduced to an acceptable minimum”.</p> <p>Need to ensure confidentiality, integrity and availability of IT systems.</p> <p>Risks include malfunctioning of information technologies, the breakdown of information infrastructure or coincidental IT failures</p> <p>Main risk is cyber attacks directed against one or several IT systems and aimed at damaging IT security:</p> <ul style="list-style-type: none"> – Attacks against the confidentiality of IT systems (“cyber espionage”) – Attacks against the integrity and availability of IT systems (“cyber sabotage”) 	<p>Strategy prepared by the Federal Ministry of Interior</p> <p>Implementation of the strategy under the overall control of a new National Cyber Security Council composed of the Federal Chancellery and state secretaries from the Foreign Office, Ministries of Interior, Defence, Finance, Economics and Technology, Justice, Education and Research, reps of States as well as the private sector as associate members</p>	<p>Ten strategic areas:</p> <ol style="list-style-type: none"> 1. The protection of critical information infrastructures as the main priority of cyber security 2. Secure IT systems in Germany 3. Strengthening IT security in the public administration 4. New National Cyber Response Centre 5. New National Cyber Security Council to enhance cooperation between Federal institutions as well as between the public and private sector 6. Effective Crime Control also in cyberspace 7. Effective coordinated action to ensure cyber security in Europe and worldwide 8. Use of reliable and trustworthy information technology 9. Personal development in Federal authorities 10. Tools to respond to cyber attacks 	<p>Strategic area #6 on Effective Crime Control also in cyberspace:</p> <ul style="list-style-type: none"> – strengthened capabilities of law enforcement, Federal Office for Information Security and private sector – joint industry/law enforcement institutions – projects to support partner countries – major effort for global harmonisation of criminal law based on Council of Europe Cyber Crime Convention examination of need for additional conventions at UN level

Country/ strategy	Vision/objectives/issues to be addressed	Institutional responsibility	Strategic priorities and measures	Measures on cybercrime
<p>India Discussion Draft on National Cyber Security Policy (2011)⁷⁶</p>	<ul style="list-style-type: none"> - Relevance of IT sector for economy. India as a global player for world-class technology and business services. - Threat of attacks and malicious use of IT by criminals, terrorists or States. - Threat of attacks against government or critical information infrastructure - Need for cyber security eco system. - Need for cyber intelligence and cyber defense. <p>“Cyber security is the activity of protecting information and information systems (networks, computers, data bases, data centers and applications) with appropriate procedural and technological security measures.”</p> <p>Priorities: Awareness, legal environment, protection, compliance, incident/emergency response, security techniques and technologies, culture of cyber security, cyber crime prevention and prosecution, data protection</p>	<p>Draft prepared by Department of Information Technology, Gov. of India</p> <p>13 types of stakeholders are listed (e.g. National Information Board, National Crisis Management Committee, National Security Council Secretariat, CERT-IN, sectoral CERTs) with a focus on incident management and response</p>	<p>3.0 Enabling processes:</p> <ul style="list-style-type: none"> - Security threat and vulnerability management - Security threat early warning and response - Security best practices, compliance and assurance <ul style="list-style-type: none"> - Critical information infrastructure protection - Information security assurance framework - E-governance - Secure software development and application - Security crisis management for countering cyber attacks and cyber terrorism - Security legal framework and law enforcement - Security information sharing and cooperation <p>4.0 Enabling technologies 5.0 Enabling people 6.0 Responsible action by user community</p>	<p>Section 3.5 Security legal framework and law enforcement:</p> <ul style="list-style-type: none"> - Legal framework - Dedicated cybercrime units - Training facilities for law enforcement and judiciary - International cooperation for information sharing and prosecution - Strategy on combating hi-tech/cybercrime: - E-crime reporting - Crime reduction and prevention - Legislation - Business-industry-public cooperation - International cooperation <p>Section 3.6 Security information sharing and cooperation</p> <ul style="list-style-type: none"> - CERT – law enforcement cooperation at domestic and international level

Country/ strategy	Vision/objectives/issues to be addressed	Institutional responsibility	Strategic priorities and measures	Measures on cybercrime
<p>Netherlands National Cyber Security Strategy, NCSS (2011)⁷⁷</p>	<p>Cyber security is defined as to be free from danger or damage caused by disruption or failure or abuse of ICT, that is, from a limitation of the availability and reliability of the ICT, breach of the confidentiality of information stored in ICT or damage to the integrity of that information.</p> <p>Action is required because:</p> <ul style="list-style-type: none"> – ICT is of fundamental importance for society and economy – Society is vulnerable (threats include botnets, attacks against infrastructure by other states (Stuxnet), denial of service attacks – Need for cooperation between parties in digital society at domestic and international levels <p>“The goal of this strategy is to reinforce the security of the digital society, in order to increase confidence in the use of ICT by citizens, the business community and government. Toward this end, the Dutch government wants to work together more effectively with other parties on the security and the reliability of an open and free digital society.</p> <p>This will stimulate the economy and increase prosperity and well-being. Good legal protection in the digital domain is guaranteed and social disruption is prevented or adequate action will be taken if things were to go wrong.”</p>	<p>Responsibility will be with a new Cyber Security Board in which all relevant parties will be represented</p> <p>A National Cyber Security Centre to be created with public and private parties</p> <p>GOVCERT.NL to be reinforced and to be placed in this Centre</p>	<p>Action lines are:</p> <ol style="list-style-type: none"> 1. Setting up the Cyber Security Board and National Cyber Security Centre 2. Preparing threat and risk analyses 3. Increasing the resilience of vital infrastructure 4. Response capacity for withstanding ICT disruptions and cyber attacks 5. Intensifying investigation and prosecution of cyber crime 6. Stimulating research and education 	<p>Action line 5 specifically addresses cybercrime:</p> <ul style="list-style-type: none"> – Expert pool and register of experts from government, private sector and academia – Focus on cross-border investigations – Focus on international legislation and regulations for cyber crime – Steering group to be established at national level for priority crime – Sufficient specialists in the entire criminal justice chain to tackle cyber crime – Public Order & Safety Inspectorate to review functioning of police – Shift of budgetary resources to enhance investigation and prosecution of cyber crime – Cyber crime programme approach: <ul style="list-style-type: none"> – Knowledge centre within the police – Reinforcement of police organisation and shift of resources – Specialised prosecutors, judges and cyber law magistrates

Country/ strategy	Vision/objectives/issues to be addressed	Institutional responsibility	Strategic priorities and measures	Measures on cybercrime
<p>South Africa Draft Cybersecurity Policy of South Africa (2010)⁷⁸</p>	<ul style="list-style-type: none"> - Need for coordinated approach in dealing with cybersecurity - Legal challenges to deal effectively with cybercrime - Need for enhanced international cooperation for cybersecurity - Business/government/civil society partnerships required to address cybercrime - Need for cybersecurity standards and protocols - The aim of the policy is to establish an environment that will ensure confidence and trust in the secure use of ICTs. - Objectives: <ul style="list-style-type: none"> - Facilitate the establishment of relevant structures in support of Cybersecurity - Ensure the reduction of Cybersecurity threats and vulnerabilities - Foster cooperation and coordination between government and the private sector - Promote and strengthen international cooperation on cybersecurity - Build capacity and promoting a culture of cybersecurity - Promote compliance with appropriate technical and operational cybersecurity standards 	<p>Draft policy developed by Department of Communications Published in the Government Gazette for public consultations</p>	<ul style="list-style-type: none"> - Creating institutional capacity to respond to cybercrime and threats <ul style="list-style-type: none"> - National Cybersecurity Advisory Council - Computer Security Incident Response Teams - Reducing cybersecurity threats and vulnerabilities - Coordinated local and international partnerships <ul style="list-style-type: none"> - Foster cooperation and coordination between government, private sector and citizens - Promote and strengthen international cooperation - Continuous innovation, skills development and compliance <ul style="list-style-type: none"> - Promote compliance with appropriate technical and operational cybersecurity standards 	<p>Cybercrime is referred to and defined as the acts covered by Chapter XIII of the Electronic Communication and Transactions Act 25 of 2002 (unauthorized access to, interception of or interference with data, including misuse of devices (Section 86), computer-related extortion, fraud and forgery (Section 87) and attempt, and aiding and abetting.</p> <p>Some general measures are foreseen in this respect:</p> <ul style="list-style-type: none"> - Development of proactive measures for the prevention and combating cybercrime - Public-private partnerships - Research and development to enhance skills to mitigate cybercrime

Country/ strategy	Vision/objectives/issues to be addressed	Institutional responsibility	Strategic priorities and measures	Measures on cybercrime
<p>United Kingdom Cyber Security Strategy (2009)⁷⁹</p>	<p>Vision is that “citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space”</p> <ul style="list-style-type: none"> – UK dependence on cyber space – Cyber space a domain where national security can be harmed (link to National Security Strategy) – Threat actors can be criminals, states or terrorists – Cyber space offers opportunities to fight cybercrime and terrorism <p>“Cyber security embraces both the protection of UK interests in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers”</p> <p>The strategic objective is to secure the UK’s advantage in cyber space by</p> <ul style="list-style-type: none"> – reducing risk from the UK’s use of cyber space (reduce the threat of cyber operations by reducing and adversary’s motivation and capability; reduce the vulnerability of UK interests to cyber operations; reduce the impact of cyber operations on UK interests) – exploiting opportunities in cyber space (gather intelligence on threat actors; promote support for UK policies, intervene against adversaries) – improving knowledge, capabilities and decision-making 	<p>Strategy presented by Prime Minister to UK Parliament</p> <p>Two new structures created:</p> <ul style="list-style-type: none"> – The Cyber Security Operations Centre as a multi-agency body to monitor developments in cyber space, analyse trends and to improve technical response coordination – The Office of Cyber Security – initially set up in the Cabinet Office – to provide strategic leadership and manage the implementation of the Strategy 	<p>Programme based on eight “workstreams”:</p> <ol style="list-style-type: none"> 1. Safe, secure and resilient systems 2. Policy, doctrine, legal and regulatory issues 3. Awareness and cultural change 4. Skills and education 5. Technical capabilities and research and development 6. Exploitation 7. International engagement 8. Governance, roles and responsibilities 	<p>Regarding the response to “e-crime”, the strategy refers to a specific cyber crime strategy prepared by the Home Office.</p>

Country/ strategy	Vision/objectives/issues to be addressed	Institutional responsibility	Strategic priorities and measures	Measures on cybercrime
<p>United Kingdom Cyber Crime Strategy (2010)⁸⁰</p>	<ul style="list-style-type: none"> - Focus specifically on cyber crime defined as new offences committed by using new technology, that is, offences against computer data and systems, and old offences committed using new technology, including fraud and financial crime, threats to children, hate crimes, harassment, political extremism and terrorism - Threat to public, business and government - Cyber crime is international crime and "the compatibility of criminal offences and investigative measures across a range of jurisdictions is as one of the most effective ways of enabling international cooperation" - Need to ensure effective and coordinated approach - Need for bringing together government, industry and the third sector 	<ul style="list-style-type: none"> - Strategy presented by Home Office to UK Parliament - Primary responsibility for action with Home Office - Close cooperation with Office of Cyber Security - Review strategy on 6-month basis to ensure consistency 	<p>This strategy is focusing on cyber crime and complements the UK's Cyber Security Strategy of 2009. Measures include:</p> <ul style="list-style-type: none"> - Enhance Government coordination to tackle cybercrime - Create a hostile environment for cybercriminals <ul style="list-style-type: none"> - Provision of reporting/recording structures (make use of experience of Action Fraud, Child Exploitation and Online Protection Centre (CEOPS), Internet Watch Foundation) - Law enforcement response (creation or strengthening of specialised units) - Technical development for law enforcement - Prosecution, financial investigations and asset recovery, review of legislation - Consumer protection - Raising public confidence <ul style="list-style-type: none"> - Financial and technical safety information - Child safety and education - Working with the private sector <ul style="list-style-type: none"> - Financial crime (e.g. e-crime partnership) - Child internet safety - International working <ul style="list-style-type: none"> - Work with G8, EU and Council of Europe on international standards for operational work, ratify Budapest Convention - Support governments to develop response to cybercrime - Law enforcement cooperation for child protection (Virtual Global Task Force) - Internet Governance Forum, ICANN and ITU - Work of Attorneys General - Global Prosecutors E-crime Network (GPEN) 	

7 References

Agence Nationale de la Sécurité des Systems d'Information [France] (2011): Défense et sécurité des systems d'information – Stratégie de la France.

http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

Australia Government - Attorney General Department (2009): Cyber Security Strategy

[http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/\(4CA02151F94FFB778ADAEC2E6EA8653D\)~AG+Cyber+Security+Strategy+-+for+website.pdf/\\$file/AG+Cyber+Security+Strategy+-+for+website.pdf](http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf)

Council of Europe (2001): Convention on Cybercrime

<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG>

Council of Europe/Committee of Ministers (1989): Recommendation No. R(89) 9 on Computer-related Crime

<https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2>

Council of Europe/Global Project on Cybercrime (2009): Cybercrime training for judges and prosecutors: a concept

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/2079_train_concept_4_provisional_8oct09.pdf

Council of Europe/Octopus Programme (2008): Guidelines for the cooperation between law enforcement and internet service providers against cybercrime

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp

Czech Republic (2011): Czech Republic (2011): Cyber Security Strategy for the Czech Republic for the 2011 – 2015 Period

http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF

ENISA (2010): Country reports – Overview

http://www.enisa.europa.eu/act/sr/files/country-reports/enisa_country_reports_introduction.pdf

European Union (2008): Council conclusions on a concerted work strategy and practical measures against cybercrime

<http://register.consilium.europa.eu/pdf/en/08/st15/st15569.en08.pdf>

Estonian Ministry of Defence (2008): Cyber Security Strategy

http://www.eata.ee/wp-content/uploads/2009/11/Estonian_Cyber_Security_Strategy.pdf

Geers, Kenneth (2011): Strategic Cyber Security (CCDCOE, Tallinn)

http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF

German Federal Ministry of the Interior (2011): Cyber Security Strategy for Germany

English version:

http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber_eng.pdf;jsessionid=365A25B8FF75170FF9566570016DDEA9.1_cid165?_blob=publicationFile

German version:

http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile

Government of Canada (2010): Canada's Cybersecurity Strategy
http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf

Government of South Africa (2010): Draft Cybersecurity Policy of South Africa
<http://www.pmg.org.za/files/docs/100219cybersecurity.pdf>

India – Department of Information Technology (2011): Discussion Draft on National Cyber Security Policy
http://www.mit.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf

Japan: Comprehensive Strategy on Information Security: Executive Summary
<http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN015121.pdf>

Ladani, Behrouz Tork/Berenjkoub, Mehdi (2006): A Comparative Study on National Information Security Strategies in Finland, US and Iran.
<http://eng.ui.ac.ir/~ladani/Papers/2006/WITID06-Comparison.pdf>

Netherlands (2011): The National Cyber Security Strategy (NCSS)
<http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011>

New Zealand Police (2007): E-crime Strategy to 2010
<http://www.police.govt.nz/resources/2007/e-crime-strategy/e-crime-strategy.pdf>

OECD (2002): Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Paris
<http://www.oecd.org/dataoecd/16/22/15582260.pdf>

UK Cabinet Office (2009): Cyber Security Strategy of the United Kingdom
<http://www.cybersecuritymarket.com/wp-content/uploads/2009/06/css0906.pdf>

UK Home Office (2010): Cyber Crime Strategy
<http://www.official-documents.gov.uk/document/cm78/7842/7842.pdf>

US Department of Defence (2011): DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE
<http://www.defense.gov/news/d20110714cyber.pdf>

US White House (2011): International Strategy for Cyberspace
http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf