CYBERSECURITY POLICY MAKING AT A TURNING POINT

Analysing a new generation of national cybersecurity strategies for the Internet economy

Also includes contributions from non-governmental stakeholders

OECD

BETTER POLICIES FOR BETTER LIVES

Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy

and

Non-governmental Perspectives on a New Generation of National Cybersecurity Strategies: Contributions from BIAC, CSISAC and ITAC

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

Cover image : © germanskydive110 - Fotolia.com

Foreword

A comparative analysis by the OECD of a new generation of national cybersecurity strategies reveals that cybersecurity policy making is at a turning point. In many countries, it has become a national policy priority supported by stronger leadership. All new strategies are becoming integrated and comprehensive. They approach cybersecurity in a holistic manner, encompassing economic, social, educational, legal, law-enforcement, technical, diplomatic, military and intelligence-related aspects. "Sovereignty considerations" have become increasingly important.

This booklet includes the OECD report as well as the full text of the contributions to this work by non-governmental stakeholders from the Business and Industry Advisory Committee (BIAC), Civil Society Internet Society Advisory Council (CSISAC) and the Internet Technical Advisory Committee (ITAC).

The OECD focuses on security in cyberspace as a driver for economic prosperity and social development. The findings of this work will inform the review of the 2002 Guidelines for the Security of Information Systems and Networks which provide a set of high level principles for addressing security in an open and interconnected digital environment through a risk-based approach.

For more information: **http://oe.cd/security**.

Table of contents

CYBERSECURITY POLICY MAKING AT A TURNING POINT

Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy

Foreword

This report analyses the latest generation of "national cybersecurity strategies" in ten volunteer countries and identifies commonalities and differences. The volunteer countries responded to a questionnaire and provided relevant material, between February 2011 and May 2012. Representatives of business, civil society and the Internet technical community participated actively in the work, in particular by responding to a questionnaire. The full text of their contribution is available in a separate document (OECD, 2012b).

The report was discussed by the Working Party on Information Security and Privacy (WPISP) and declassified by the Committee for Information, Computer and Communications Policy (ICCP) at its 64th session on 24 October 2012. The findings of the work will inform the upcoming review of the OECD 2002 *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*.

The report was prepared under the direction of a group of delegates led by Geoff Smith (United Kingdom) and Manuel Pedrosa de Barros (Portugal) by Laurent Bernat (OECD Secretariat) with Peter Ford and Nick Mansfield, consultants to the OECD.

OECD work on cybersecurity can be found at **http://oe.cd/security**.

Main points

The comparative analysis of a new generation of national cybersecurity strategies in ten OECD countries reveals that cybersecurity policy making is at a turning point. In many countries, it has become a **national policy priority** supported by stronger leadership. A single definition of cybersecurity cannot be derived from these strategies. Nevertheless, all new strategies are becoming **integrated** and comprehensive. They approach cybersecurity in a holistic manner, encompassing economic, social, educational, legal, law-enforcement, technical, diplomatic, military and intelligence-related aspects. "**Sovereignty considerations**" have become increasingly important.

The new generation of national cybersecurity strategies aims to drive economic and social prosperity and protect cyberspace-reliant societies against cyber-threats. This has been a traditional area of interest for the OECD, going back to the 1992 Guidelines for the security of information systems. A key challenge of cybersecurity policy making today is to pursue these two objectives while preserving the openness of the Internet as a **platform for innovation and new sources of growth**.

Cybersecurity strategies recognise that the economy, society and governments now rely on the Internet for many essential functions and that cyber threats have been increasing and evolving at a fast pace. Most strategies aim to enhance governmental co-ordination at policy and operational levels and clarify roles and responsibilities. They reinforce public-private co-operation. They emphasise the need to respect fundamental values such as privacy, freedom of speech, and the free flow of information. They also call for improved international co-operation. Some strategies also support more flexible and agile policy approaches, and emphasise the economic dimension of cybersecurity policy. Some create the conditions for a multistakeholder dialogue in the cybersecurity policy making and implementation process.

Action plans strengthen key priority areas identified in the early 2000s. They include more emphasis on cybersecurity research and development (R&D) and real time monitoring of government infrastructures. They aim to develop a more robust cybersecurity industry sector and to take advantage of economic drivers and incentives for cybersecurity. They identify critical business actors or sectors to the economy. They create partnerships with Internet Service Providers and encourage cybersecurity exercises. They

develop digital identity frameworks and specific policies for the protection of children on line.

In addition to describing this evolution of cybersecurity policy making, the report highlights suggestions by business, civil society and the Internet technical community, for example with respect to security-related barriers to trade that could inhibit innovation and global deployment of cost-effective security solutions. The report calls for further analysis of the intersections between economic, social and sovereignty cybersecurity policies and points out the opportunity for countries to extend their national co-ordination agency as an international contact point to facilitate co-operation on cybersecurity at policy and operational levels. It also makes suggestions in the context of the review of the 2002 OECD *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* ("Security Guidelines").

This new age of cybersecurity policy making is still in its infancy and will take time to further develop. In the meantime, a key challenge for governments is to be prepared to face a possible serious cyber incident, as envisaged in nearly all the strategies, in a way that does not undermine the **openness of the Internet** which is key to the vitality of the Internet economy.

Synthesis

This report analyses the emergence of a new generation of government policies, sometimes called "cybersecurity strategies", in a total of ten volunteer OECD countries: eight which had adopted such a strategy between 2009 and the end of 2011 (Australia, Canada, France, Germany, Japan, Netherlands, the United Kingdom and the United States), and two which were in the process of developing one (Finland and Spain). It is based on the responses to a questionnaire (annex V), the analysis of the strategies themselves and additional research carried out by the Secretariat.[1] The report explores areas of commonalities and differences across countries and identifies key changes between this new generation of policies and previous governmental efforts as analysed by the OECD in 2004 (OECD, 2005). It also reflects considerations and suggestions expressed by non-governmental stakeholders[2] in their response to a questionnaire circulated in January 2012 (see annex VI: the responses of non-governmental stakeholders are available separately). Finally, the report draws some conclusions on the role of the OECD and the review of the 2002 OECD Security Guidelines. Several annexes provide more details, for example with respect to intergovernmental organisations involved in cybersecurity (Annex I), and developments in the European Union (Annex II).

Cybersecurity has become a national policy priority

The analysis of this new generation of national cybersecurity strategies reveals a fundamental evolution in government policy making whereby cybersecurity is elevated among government priorities. According to these strategies, governments' general assessment is that:

- *The Internet and ICTs are essential for economic and social development and form a vital infrastructure*. In a general context of economic downturn, the open Internet and ICTs are a new source of growth and a driver for innovation, social well-being and individual expression. As the Internet economy grows, the whole economy and society, including governments, become increasingly reliant on this digital infrastructure to perform their essential functions.

- *Cyber threats are evolving and increasing at a fast pace*. They are still initiated by criminal actors but also come from new sources, such as foreign states and political groups, and may have other motivations than money making, such as some types of "hacktivism" (Anonymous), destabilisation (Estonia in 2007), cyberespionage, sabotage (*e.g.* Stuxnet) and even military operations. Malicious actors are better organised, in particular to conceal their tracks, and the degree of sophistication has increased significantly, showing clear signs of professionalisation.

As a consequence, the scope of almost all new cybersecurity strategies has evolved from solely protecting individuals and organisations as distinct actors, to also protecting society as a whole. This change results from the evolution of the role of the Internet in society. When the Internet was merely a *useful* platform for individuals and organisations, the consequences of failures were manageable at the level of each individual and organisation, and government policy was about helping them to prevent and manage such incidents. As the Internet has become *essential* for the economy and the society, the consequences of failures can directly impact society as a whole. Therefore, cybersecurity strategies aim at achieving two interrelated objectives: strengthening cybersecurity for the Internet economy to further drive economic and social prosperity, and protecting cyberspace-reliant societies against cyber-threats. Managing the complexity of pursuing these two objectives in parallel, while preserving the openness of the Internet and fundamental values, is probably the main challenge of cybersecurity policy making today.

The criticality of the Internet for the modern economy has several consequences on cybersecurity policy making, the main one being the adoption of strategies that approach cybersecurity in an **integrated and comprehensive manner**. Governments recognise the need to address all the facets of cybersecurity holistically rather than in a fragmented manner as in the past. New cybersecurity strategies are government-wide and encompass the economic, social, educational, legal, law-enforcement, technical, diplomatic, military and intelligence-related aspects of cybersecurity. This integrated approach is generally supported by **strong leadership**, sometimes at head of state or head of government level, illustrating the significant elevation of cybersecurity amongst government priorities.

Not all strategies use the terms of "cyberspace" and "cybersecurity". Some of those which use these terms also provide a definition which varies across countries. Most countries include the concept of critical information infrastructures in the scope of their strategy, as defined in the OECD *Recommendation on the Protection of Critical Information Infrastructures.*[3]

Some concepts are shared by all strategies

Most strategies share the following concepts:

- *Enhanced governmental co-ordination at policy and operational levels*. As cybersecurity becomes an issue of national priority, responsibility for cybersecurity policy making and implementation is being clearly assigned within the government. However, no single existing vertical agency can claim a comprehensive understanding and a sufficiently wide authority to manage all facets of cybersecurity. Thus, co-ordination among the relevant bodies becomes essential. The responsibility for co-ordination is generally assigned to a specific existing or new agency, and the responsibility of the other government bodies involved is also clearly assigned, to facilitate co-operation, encourage synergies, avoid duplication, and pool initiatives. Again, this evolution from a *multi-agency* to an *inter-agency* approach requires strong leadership to enable co-ordination and co-operation across pre-existing government silos. Specific arrangements vary across countries and reflect cultures and styles of government.

- *Reinforced public-private co-operation*. All strategies recognise that cyberspace is largely owned and operated by the private sector and that users also play a key role. They acknowledge that policies must be based on inclusive public-private partnerships, which may include business, civil society, the Internet technical community, and academia. However, the modalities of such consultations and the level of detail provided in the strategies vary.

- *Improved international co-operation.* International co-operation and the need for better alliances and partnerships with like-minded countries or allies, including facilitating capacity building of less developed countries are shared as key objectives by most strategies. Most countries, however, provide little detail on how to achieve enhanced international co-operation. Exceptions include the United States which has developed a specific international strategy for cyberspace, and the United Kingdom which initiated an international dialogue at the 2011 London Conference on Cyberspace and promoted the concept of international norms of behaviour in cyberspace which can also be found in the Australian and German strategies. The need for a higher degree of harmonisation of legislation against cybercrime is often pointed out, generally in support of the 2001 Budapest Convention on Cybercrime. International and regional organisations such as the Council of Europe, the European Union, the G8, the Internet Governance Forum, the OECD, the Organisation for Security and Co-operation in Europe

(OSCE) and the United Nations, including the International Telecommunications Union (ITU), are mentioned but without much detail as regards their role, except for the North Atlantic Treaty Organisation (NATO), mentioned by several countries with respect to cybersecurity in the military context.[4]

- *Respect for fundamental values*: all strategies place a strong emphasis on the need for cybersecurity policy to respect fundamental values, which generally include privacy, freedom of speech, and the free flow of information. Several strategies explicitly mention the need to maintain the openness of the Internet and no strategy suggests modifying it in favour of strengthened cybersecurity. On the contrary, the openness of the Internet is generally described as a requirement for the further development of the Internet economy.

Other concepts may reveal emerging trends

Analysis of the strategies enables the identification of other key concepts which are not necessarily expressed by all countries, but nevertheless indicate possible new trends. Most strategies place a particular emphasis on:

- Sovereignty considerations in cybersecurity policy making, *i.e.* national and international security, intelligence, defense and military aspects

  This evolution is a direct consequence of the consideration that cybersecurity addresses the protection of the society as a whole and requires a whole of government integrated approach. Sovereignty considerations emerge at different levels of domestic policy: *i) at the strategic level*, for example with the recognition of cyber threats targeting the military, or the risk of cyberespionage from foreign states, *ii) at the organisational level*, as departments and ministries in charge of diplomacy, intelligence and the military are included in the intergovernmental co-ordination for policy making, sometimes with a "national security" inter-agency body being assigned overarching responsibility for cybersecurity co-ordination, *iii) at the operational level*, with, for example, intelligence bodies playing a key role as a source of information for situational awareness. Sovereignty considerations also appear at the international policy level: *i)* strategies mention the need for an international dialogue in relation to "rules of engagement" in cyberspace or "confidence building measures", *ii)* they highlight the role of some organisations like NATO and OSCE to address these issues, and *iii)* they mention operational co-operation with respect to intelligence-related information sharing between allies.

- Flexible policy approach

  The Internet economy is a dynamic environment where technologies, usages and markets constantly evolve in an unpredictable manner for the benefit of economic growth and innovation, and where threats are also in permanent evolution. Several strategies promote flexible and agile cybersecurity policies which preserve the openness of the Internet and the free flow of information as well as other factors that enable the Internet to generate economic and social benefits and accommodate a fundamentally dynamic environment. Several strategies support policies that enable fast and informed decision-making processes, embed rapid feedback mechanisms and include efficient learning cycles and improvement to quickly and efficiently implement new measures. Some strategies consider that self-regulation should be favoured and legislation considered only in cases where self-regulation is not possible or not effective.

- The importance of the economic aspects of cybersecurity

  While all strategies aim to address cybersecurity in order to maintain and further develop economic and social prosperity through the continued development of a vibrant Internet economy, the economic aspects of cybersecurity are gaining increased visibility in several strategies. Some countries highlight that a higher level of cybersecurity will provide their economy with a competitive advantage. They recognise that economic factors play a key role in improving cybersecurity. Several strategies encourage flexible policies leveraging incentives for markets to better take security into account. Some require better understanding of the incentive structure of market players in relation to cybersecurity and promote lightweight measures such as encouraging the use of security labels applied to products and services to better inform the market. Several countries set as a key policy objective the development of a stronger cybersecurity industry sector, including the development of a larger cybersecurity workforce. They also mention the possible development of a cybersecurity insurance sector. Some strategies identify a higher degree of technological independence in relation to IT security as an important policy objective.

- The benefits of a multistakeholder dialogue

  Many strategies share the view that dialogue with non-governmental stakeholders is key to good cybersecurity policy making and implementation. However, the level of detail with regards to whether and how governments engage into a multistakeholder dialogue varies, with many strategies providing little or no details on this aspect. Some

strategies establish a dedicated body including these stakeholders to provide information and advice to the government. In general, input from business is widely recognised as essential, including for the implementation of the strategies, but less information is available as regards the consultation with the civil society, beyond academia.

Actions plans are reinforced and broadened

Cybersecurity strategies generally include or are followed by the adoption of action plans aimed to strengthen key priority areas which were identified in the survey carried out in 2004:[5]

- *Government security*: action plans include a multiplicity of initiatives, from the development of a situational awareness capacity to the rationalisation of government network infrastructures, and the generalisation of audits in the public sector.
- *Protection of critical information infrastructures*: action plans generally include measures related to the protection of critical information infrastructures.
- *Fight against cybercrime*: action plans include many initiatives to develop law enforcement capacities, improve the legal framework and foster international co-operation on the basis of the Budapest Cybercrime Convention.
- *Awareness raising*: action plans include many initiatives targeting specific populations such as children, SMEs and decision makers in government and critical infrastructures.
- *Education*: action plans recognise in particular the need for a stronger cybersecurity workforce. The development of cybersecurity skills is identified as a key priority by several countries.
- *Response*: strategies recognise the role played by Cyber Security Incident Response Teams (CSIRTs), and create a national CSIRT or strengthen it where it already exists.

Research and Development (R&D), which benefited from a relatively low level of attention in an OECD survey carried out in 2004 is elevated to a much higher level of priority in new cybersecurity strategies, generally focusing on better organisation and co-ordination of existing cybersecurity R&D efforts in partnership with the private sector. One country, the United States, adopted a strategic plan for its cybersecurity R&D programme.

Some cybersecurity strategies also introduce new themes in their action plans such as:

- The development of a situational awareness and real time monitoring capacity, mainly for government infrastructures.
- The development of policies to support the development of a more robust cybersecurity industry sector.
- The consideration of specific business players or sectors which, without strictly being defined as critical information infrastructures, could cause significant damage to the economy if successfully targeted.
- Partnerships with Internet Service Providers (ISPs) to address the botnet threat, with the participation of their customers.
- The identification of economic drivers and incentives such as data breach notification frameworks or labelling schemes on products and services.
- Cyber security exercises, including across borders.
- The development of digital identity frameworks.
- Specific policies for the protection of children on line.

Considerations expressed by non-governmental stakeholders

This section reflects some of the observations and suggestions expressed by business, civil society and the Internet technical community[6], in response to a questionnaire circulated in January 2012 about the current evolution of cybersecurity policy making (cf. Annex VI).

Generally, non-governmental stakeholders agree that *i)* multistakeholder collaboration and co-operation are the best means to develop effective cybersecurity policies that respect the fundamentally global, open and inter-operable nature of the Internet; *ii)* policy options must be flexible enough to accommodate the dynamic nature of the Internet; *iii)* more robust evidence-based cybersecurity policy making is needed, an area which is generally not covered by cybersecurity strategies.

Non-governmental stakeholders consider that the divide between **sovereignty and economic/social cybersecurity** policy making is increasingly blurred and that this trend could lead to challenging consequences. For example, business points out that it could face additional burdens while civil society is concerned that its consultative role could be reduced, that transparency could decrease and that warfare semantics could increasingly shape the cyber-

security policy debate, with the risk of minimising the economic and social benefits of the openness of the Internet.

In addition to greater consultation with non-governmental stakeholders, civil society suggests several measures to ensure that cybersecurity policy making remains transparent, proportionate and balanced. For example, cybersecurity strategies could include a sunset clause to prevent measures which were legitimate at the time of their adoption from threatening fundamental rights as technology evolves. Policy initiatives could systematically include a clear risk assessment detailing the specific harm that they plan to address as well as an assessment of their impact on fundamental rights such as free flow of information, privacy and freedom of speech.

A number of other proposals are put forward by stakeholders to **increase the effectiveness of cybersecurity strategies**. For example,

- The consistency of cybersecurity measures with other cybersecurity initiatives could be systematically assessed (civil society). For example, legislation which criminalises hacking could take into account that legitimate research contributing to enhance cybersecurity may employ the same techniques.
- Governments as owners and operators of information systems and networks could lead by example by adopting best practices, technologies and even legislative requirements. Appropriate trust compliance programmes and procurement practices by government can provide a clear direction to other economic actors. Technologies developed for the government can also benefit the market (civil society, Internet technical community).
- Policy makers could seek advice from the Internet technical community as early as possible in the policy making process to avoid pursuing technologically flawed decisions (Internet technical community).
- Policies could encourage the development of open standards enabling innovation for security solutions, relying on respected and well-established open Internet standardisation groups and avoiding unilateral modification of Internet standards (Internet technical community).
- The collection of empirical evidence could be encouraged to better assess the relevance of strategies and policies, as well as to support the risk-based approach called for in the Security Guidelines. Various means for increasing evidence-based policy making have been highlighted to counterbalance existing disincentives that many players face in providing more information regarding cyber incidents. They

include harmonised breach notification mechanisms and the disclosure of metrics related to risks faced by government systems (civil society, Internet technical community).

Finally, the **international dimension** of cybersecurity policy making is highlighted by business and the Internet technical community. They stress that requirements imposed by some countries on ICT equipment create complex challenges for the industry. They underline that security-related technical barriers to trade, for example in the form of local standards requirements, redundant security certification schemes or interferences in the global value chain increase cost, limit functionality, constrain innovation, and skew a level playing field. They call for government policies to allow for the deployment of global cost-effective industry solutions and encourage the exploration of solutions, for example through international standards, cross-compliance recognition frameworks and awareness raising of less developed countries on this issue.

The review of the Security Guidelines

The 2002 Recommendation of the OECD Council concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security (the 2002 Security Guidelines) established the first international set of fundamental principles focused on the development of security policies in an open environment. They can be used by governments to develop national policies as well as by public and private organisations to design their own security policies. The comparison of national cybersecurity strategies provides a useful source of information and inspiration in the context of the review of the Guidelines initiated in 2012.

All the strategies studied are consistent with the Guidelines' principles and several directly reflect some key concepts such as the need for a culture of (cyber)security, the shared responsibility of all participants and the need for a risk-based approach. Nevertheless, none of these strategies explicitly mentions the OECD Security Guidelines. This might be interpreted as a proof of success, considering that the Guidelines' principles have become so universal that policy makers do not feel the need to reference them. It could also raise the issue of the capacity of a ten year old Recommendation to maintain momentum in such a fast evolving area and of the OECD to retain ownership of one of its successful policy achievements.

While it is straightforward to identify the Guidelines' principles in the strategies, the analysis of the latter shows that two prominent concepts may be identified as missing in the Guidelines: resilience and real-time.

Resilience is used in many national strategies, without a clear definition but generally as the capacity of an information system or network to continue to operate despite incidents, or to carry on normal operations smoothly notwithstanding technical problems. The notion of resilience or, more broadly, of "business continuity" implies that in an open environment, some level of risk has to be accepted and that one should be prepared for incidents to occur. It is therefore consistent with a security approach based on risk assessment and management as promoted by the Security Guidelines and relates to several principles such as Response (3), Risk Assessment (6), Security Design and Implementation (7), and Security Management (8).

Real-time capacity appears in most strategies, even if not explicitly, as an extension of the concept of "timeliness" included in the Guidelines' Response principle. Although governments have established or strengthened national Computer Security Incident Response Teams (CSIRTs), they generally recognise the need for more real-time "situational awareness" at operational level. Governments achieve this notably through the establishment of Cyber Security Operation Centers (CSOCs) for the security of their own networks. The need for real time cybersecurity management is also reflected in the private sector with increased demand for such CSOC solutions. The emergence of real-time capacity in cybersecurity is consistent with the recognition that, in an open and interconnected environment, security controls will not be robust enough to fully control a perimeter that can potentially extend to the whole Internet. This implies that risk management measures take into account the possibility that unauthorised entities gain access to the system with malicious intentions, and that measures to detect and control them within the perimeter are as essential as measures to secure the perimeter. In this context, cybersecurity no longer just requires timely response to incidents, but also real-time monitoring of networks. And beyond technical security controls, the need for real-time cybersecurity management also raises challenges with respect to security processes and human decisions.

There may therefore be scope to better reflect the need for real-time cybersecurity management in the review of the Security Guidelines. This could impact, for example, the language used in the Response principle. In so doing, it would be necessary however to keep in mind challenges raised by real-time monitoring of networks for enhanced response, such as with respect to privacy and other fundamental values expressed in the Ethics and Democracy principles.

Unlike their predecessor adopted in 1992, the 2002 Security Guidelines do not include a section on how to implement the Guidelines' principles in public policy, or in public or private organisations. The common elements of current cybersecurity strategies provide several concepts that could inspire the development of such guidance *with respect to national policy making*

such as *i)* the adoption of a strategic approach, *ii)* supported by strong leadership, *iii)* addressing cybersecurity in a holistic manner, including efficient co-ordination mechanisms adapted to the country's culture and style of government, *iv)* involving non-governmental stakeholders, *v)* fostering flexible policy solutions, *vi)* encouraging self-regulation and public-private partnerships, *vii)* respecting fundamental values with appropriate safeguards and checks and balances, *viii)* and fostering international co-operation such as through the adoption of common norms of behaviour in cyberspace. And, last but not least, adopting policy measures that encourage the production of robust and internationally comparable data could be considered. This would enable better informed policy making and improve risk assessment at a macro level. Both could improve the effectiveness of government policies.

At a more operational level, the guidance could encourage the adoption of a toolkit of measures for governments, to be further refined and developed, including *i)* leading by example through the implementation of best practices for the security of their own systems and networks, *ii)* developing or, if it already exists, strengthening a national CSIRT capacity, *iii)* strengthening the fight against cybercrime, *iv)* implementing the OECD Recommendation on the Protection of Critical Information Infrastructures, *v)* raising awareness of all participants, *vi)* leveraging the appropriate incentives to stimulate the development of a cybersecurity industry sector and encouraging the development of a cybersecurity workforce, *vii)* encouraging cybersecurity research and development, *viii)* establishing a single point of contact for international co-operation, *ix)* encouraging the organisation of cybersecurity exercises, including across borders.

Conclusion

The emergence of sovereignty considerations in cybersecurity strategies is an evolution that is likely to influence policy making in the longer term. At this stage, sovereignty considerations are kept separate from the economic and social aspects of cybersecurity but intersections are becoming visible. For example, in some cases, policy and/or operational co-ordination is led by agencies whose missions focus on sovereignty considerations; some strategies call for facilitating technology spillovers from the intelligence community to the cybersecurity industry sector; new industry suppliers and products benefitting from R&D investments driven by sovereignty considerations are entering the cybersecurity marketplace; and finally, in some countries, the military and intelligence communities are becoming important potential suppliers of cybersecurity jobs. Understanding the implications of this cross-fertilisation in the short, medium and longer term might become increasingly relevant to inform the cybersecurity policy making process.

The establishment by national strategies of points of co-ordination within governments creates an opportunity to enhance international co-operation at policy and operational levels. Each country might consider extending this co-ordination effort by nominating an **international point of contact** in its government, which would be available, for example, to facilitate the distribution to the relevant domestic agencies of cybersecurity related requests from foreign countries, whether at policy or operational levels, whether for emergency, informational or other purposes.

Although the protection of critical information infrastructures is generally included in the scope of the strategies, the issue of **cross-border interdependencies** is rarely addressed at strategic level. Further co-operation on this matter, which is addressed in the OECD Recommendation on the Protection of Critical Information Infrastructures (2008), would be of mutual interest.

More generally, cybersecurity policy making seems to be reaching a **new level of maturity** as compared to previous policies rooted in the early 2000s, with stronger leadership, enhanced visibility within governments, better co-ordination, and broader involvement of stakeholders. At the same time, policy making challenges are multiplying, suggesting that governments are also facing a **new level of complexity**. For example, governments have to simultaneously address the need for more co-ordination across agencies through a higher degree of centralisation whilst enabling dynamic and fast – close to real-time – decision-making processes at all levels. Another complex challenge is the need for holistic approaches which take into account sovereignty and economic/social concerns, the involvement of a large range of government bodies, and increased co-operation with the private sector. A further challenge is the need to preserve the openness of the Internet and fundamental values, consistent with the 2011 Recommendation of the Council on Principles for Internet Policy Making. Finally, the lack of details as regards the various measures adopted, the lack of metrics and methodologies for assessing their efficiency, the rapid pace adopted by some countries in the revision of their new framework, among other factors, suggest that this new age of cybersecurity policy making is **still in its early days**.

Refining and implementing these new policy packages will take time. In the meantime, a key challenge for governments is to be prepared to face a possibly serious cyber incident, as envisaged in nearly all the strategies, in a way that does not undermine the openness of the Internet. As cybersecurity policy develops, a key question will be whether and how governments make the protection of the openness of the Internet an integral part of cyber-security.

What should be the role of the OECD?

As noted above, cybersecurity strategies recognise international organisations as essential for the improvement of international co-operation in general. They do not however provide much detail on the specific role that each of these international organisations should play. More generally, it is unclear at this stage how international co-operation on cybersecurity will evolve in the mid to long term. This includes, for example, the translation at the international level of the domestic evolution towards holistic approaches that bring together economic, social and sovereignty aspects.

In the short term, a plausible scenario is that at the request of their memberships, each forum build on its core mandate and competencies to strengthen its expertise. Countries can encourage enhanced co-operation and partnerships between organisations with complementary expertise to avoid duplication of efforts and enable synergies. In parallel, and building on this process, multilateral dialogues such as the 2011 London Conference on Cyberspace and its successors in Budapest and Korea, can foster the emergence of a broader consensus.

The OECD started to analyse the impact of ICTs on the economy and the society and to develop ICT-related policy instruments in the mid-1970s. In 1980, the OECD adopted the Privacy Guidelines, the first international policy instrument to address ICT policy in relation to trust and confidence. Since the early 1990s, the OECD has accumulated a vast amount of expertise in security of information systems and networks and other related areas including electronic authentication, cryptography policy and the protection of critical information infrastructures. So far, the OECD's approach to security in the digital world has aimed to develop security policy frameworks that enable ICTs and the Internet economy to capture new sources of growth, to foster innovation and to enhance social well-being. The OECD's main assets as reflected in the 2002 Security Guidelines (see below) are its capacity to develop recommendations based on high-level flexible policy principles, through a consensus-based process involving all stakeholders.

The trends revealed by the above analysis suggest at least two additional areas for further OECD study. The first one is related to policies fostering the development of a cybersecurity industry sector which would drive growth and employment directly, in addition to, indirectly, sustaining trust in the Internet economy (towards an "industrial cybersecurity policy"). The second one is the development of more robust and internationally comparable cybersecurity indicators, to better inform the cybersecurity policy making process as well as the market place, and would support the development of cybersecurity as a more robust economic sector.

Detailed comparative analysis

In 2003 and 2004, the OECD carried out a survey to examine how governments undertook the implementation of the 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security ("Security Guidelines"). The results of this survey highlighted that almost all governments had finalised their national strategy for fostering a culture of security (OECD, 2005). Between 2009 and 2011, several countries adopted or initiated the development of a new generation of strategies, sometimes called "cybersecurity strategies". This detailed comparative analysis explores the contextual elements that are driving the policy changes (rationale and scope) and analyses key concepts of national cybersecurity strategies. It is followed by an analysis of the management structures and key aspects of concrete plans of action for achieving strategic objectives. The third section reflects some of the considerations highlighted by non-governmental stakeholders in response to a questionnaire on national cybersecurity strategies. Finally, the last section provides other elements for discussion.

Rationale and scope

The development and adoption of new national cybersecurity strategies is an emerging trend characterised by its dynamism.

Eight of the ten countries which volunteered to participate in this comparative exercise have adopted a new cybersecurity strategy. Two other countries have initiated a process for adopting one in the short term (Finland, Spain[7]) and a European Internet Security Strategy is planned for autumn 2012.[8]

Most participating countries which adopted a strategy between 2009 and 2010 are already in the process of reviewing it. The United Kingdom which adopted a cybersecurity strategy in 2009 released a new strategy in November 2011. At the time of writing, the Australian 2009 Cyber Security Strategy was in the course of being updated by the release of the government's Cyber White Paper, following up on a public consultation carried out in autumn 2011. The rapid pace of renewal and revision of these policies indicates the emerging and fast-evolving nature of the subject matter as well as governments' willingness to take into account a rapidly changing environment through an iterative and relatively dynamic policy approach.

All strategies result from the recognition of increased cyber risks, i.e. increased cyber threats, vulnerabilities and potential impact on the economy and the society.

Traditionally, risk is defined as the potential for *threats* to exploit *vulnerabilities* generating detrimental *consequences*. According to information provided in the strategies themselves, the elevation of each of these dimensions of risk is the main driver for countries' decisions to review their approaches.

- Sources, motivations, nature, organisation and sophistication of threats are evolving…

States are emerging as new *sources* of threats in addition to individuals and groups which can be related to organised criminality, potentially to terrorism, but also to economic and commercial interests. Some strategies highlight that the distinction between traditional categories of threat sources is increasingly blurred. Political activity (some types of "hacktivism", and so-called "patriotic hackers") and problems between States are identified as new *motivations*, in addition to money and vandalism. Some strategies highlight that criminals, terrorists, intelligence services and militaries benefit from the borderless nature of the Internet which impedes the easy attribution of malicious digital activities to specific individuals.

The *nature* of threats continues to include criminal activities such as theft (of identity, personal data, secrets of all kind and financial assets), infringement of intellectual property rights, denial of service, defacement and other sources of disruption, covering breaches of confidentiality, integrity and availability. However, the main emerging types of threats are large-scale denial of service attacks, leakages of private information, cyberespionage against governments and critical parts of business and industry, and the disruption of critical infrastructures. For example, France considers that a large scale cyber-attack against national infrastructure is among the major threats the country will face in the next 15 years (ANSSI, 2011). Cyber-espionage, military operations, sabotage and deception operations are included as potential threats in many strategies. Most strategies recognise key milestones have been recently passed in most of these areas. Examples include the 2007 massive attack on Estonian networks, the 2009 large scale denial of service attacks against Korea and the United States, numerous sophisticated cyberespionage activities targeting numerous governments, regional and international institutions and firms operating in the security sector, data leakages affecting 77 and 35 million customers of respectively Sony and SK Comms. The alleged physical disruption of the Iranian nuclear enrichment programme using the Stuxnet worm is sometimes highlighted as an important

turning point in relation to the protection of critical infrastructures. The disruption of supply chains is also pointed out by some countries as an emerging threat. Finally, the UK 2011 cybersecurity strategy mentions as potential threats the possibility for States to spread disinformation and for terrorists to spread propaganda, radicalise potential supporters, raise funds, communicate and plan (UK Cabinet Office, 2011a).

The level of *organisation* of the major threat sources, whether individuals, groups or States has significantly increased. Criminal groups, motivated by financial gain, export to the virtual world their real world organisational skills in order to maximise the benefits from digital criminal activities. Even isolated individuals have developed "loose coalitions" or "decentralised online communities" to carry out disruptive activities (*e.g.* "Anonymous"). "Hacktivists" such as Lulzsec have also undertaken similar modes of organisation.

The level of *sophistication* of the threat has also significantly increased through the progressive professionalisation of these actors. For example organised criminal groups and State actors have become capable of developing extremely innovative malicious software[9] (malware) capable of evading advanced detection software. These actors have shown highly advanced skills for example to reverse engineer proprietary software in order to identify unknown "zero day" vulnerabilities. They have launched precisely targeted attacks[10] blending all sorts of complex techniques (*e.g.* Stuxnet) and accumulated considerable denial of service capacity by creating massive botnets of hundreds of thousands and, sometimes, millions of compromised computers. Similarly, tech-savvy but not necessarily highly experienced isolated individuals have benefitted from sophisticated turnkey malware packages and penetration toolkits ready to use against poorly protected targets.

In general, recent national strategies focus on evolutions related to intentional threats to describe their rationale and do not place particular emphasis on accidental threats, such as natural disasters. They recognise that motivations and intentions are the main differentiators as targets and methods of attacks may be similar. They also recognise the constantly evolving nature of the threat, sometimes making a parallel with bacteria developing drug resistance to antibiotics[11].

- ... Countries' vulnerability and reliance on ICTs and cyberspace have increased to the point where cybersecurity becomes a national priority.

Over the last ten years, the Internet evolved from a useful communication tool for individuals and organisations to an essential digital infrastructure for the economy and society as a whole. This is illustrated by the dependence of critical infrastructures on information systems and networks,[12] including for

example distribution of food, water, energy, telecommunications, transport, health service, the financial system and the functioning of all areas of government including emergency services and the military. Strategies recognise the estimated and potential losses for individuals and organisations resulting from cyber threats, for example in terms of financial damages (*e.g.* cost of cybercrime). However, they place a much greater emphasis than in the past on the dependence of the society as a whole on the digital infrastructure.

According to the United Kingdom, the reliance of the country's interests on cyberspace is "far-reaching, affecting the individual citizen, almost all aspects of government, industry, our national infrastructure, transportation and the way our economy operates" (UK Prime Minister, 2009). For Spain, much of the country's stability and economic prosperity will depend on the security of its cyberspace. According to France, the current level of attacks on information systems reveals a high potential for destabilisation of daily life, disruption of networks that are critical to the life of the nation and denial of functioning of military capacity (French Government, 2008). For the Canadian Minister of Public Safety, Canada's increasing reliance on cyber technologies makes the country vulnerable to those who attack its digital infrastructure to undermine its national security, economic prosperity and way of life (Government of Canada, 2010). The United States stresses that cyberspace provides a "platform for innovation and prosperity and the means to improve general welfare around the globe" that "touches practically everything and everyone". "For all nations, the underlying digital infrastructure is or will soon become a national asset" (US White House, 2011a). Australia recognises that its national security, economic prosperity and social wellbeing are critically dependent upon the availability, integrity and confidentiality of a range of information and communications technologies (Australian Government, 2009). The strategy cites examples such as the disruption of electric power systems in multiple regions resulting in some instances in a major multi-city power outage. The Netherlands notes that the continuity and security of supply are essential for the private sector's survival and for the society as a whole and that a breakdown could lead to social disruption (Dutch Ministry of Security and Justice, 2011).

Cybersecurity strategies aim at two interrelated objectives: protecting the society against cyber threats as it becomes more reliant on cyberspace and fostering cybersecurity as essential for the further development of the Internet economy.

- While new strategies often result from a "national security" review…

In contrast with the previous generation of strategies in the early 2000s, one of the key drivers for the development of new cybersecurity strategies is related to "national security".

For example, the French 2010 strategy on "Defense and security of information systems" results from the adoption of a 2008 "White Book on Defense and National Security" which aimed at developing a new holistic national security strategy taking into account changes in the global environment since 1994. The United Kingdom developed its 2009 strategy as a result of a change in its approach to national security initiated in 2008. The main driver for the development of the cybersecurity strategy was the identification of the increasing importance of cyberspace in the life of the United Kingdom and as one of the highest priorities for action in relation to national security. After the adoption of the strategy and the change of government, both the National Security Strategy and the Strategic Defence and Security Review (SDSR) addressed cyber security risks (2010). The 2009 Australian cybersecurity strategy was preceded by an "E-Security National Agenda" announced in 2001 and reviewed in 2006. As a result, the strategy starts with the Australian Prime Minister's statement that cyber security is now one of the country's top tier national security priorities. The planned Spanish and Finnish cybersecurity strategies will result respectively from the 2011 Spanish Security Strategy which includes a section on cyber-threats, and the 2010 Finnish National Security Strategy for Society.

In the early 2000s, cybersecurity policy making aimed to foster trust on line in order to create the conditions for the Internet to drive prosperity, growth and well being. A decade later, governments are facing a different situation: the Internet economy became a significant source of growth in its own right and a platform for innovation that cuts across all other economic sectors. Large segments of the core fabric of the economy and society rely on the Internet and related ICTs.[13] However, the Internet did not succeed because the infrastructure became more secure but rather despite its inherent insecurity. The nature of technical vulnerabilities of information systems interconnected through the Internet have not fundamentally changed. The Internet continues to be "driven more by considerations of interoperability and efficiency than security" (US White House, 2009). What has changed is that the society and the economy now rely on this fundamentally insecure

environment. Thus addressing cybersecurity has become a national priority for governments and requires a strategic approach focusing on the protection of the society as a whole rather than only on the individual interests of specific participants considered separately. This is the meaning of "national security" across all these new cybersecurity strategies and it represents a major policy evolution from the mind-set that drove the adoption of the 2002 Security Guidelines and subsequent implementation frameworks.

- … they also address cybersecurity as essential for the development of the Internet economy.

It would, however, be misleading to conclude that these countries have abandoned the economic and social objective of cybersecurity policy making. Rather, what emerges from these recent strategies is the dual objective of fostering cybersecurity for creating the conditions for a prosperous Internet economy while protecting the society as a whole from cyber risks stemming from increased reliance on cyberspace. Managing the complexity of pursuing this double objective can be seen as one of the main, if not the main, current cybersecurity policy making challenges.

For example, the German strategy aims to maintain and promote economic and social prosperity and stresses that ensuring cybersecurity has turned into a central challenge for the state, business and society and a vital question for the 21st century. The Dutch strategy focuses on strengthening the security of the digital society in order to give individuals, businesses and public bodies more confidence in the use of ICT while recognising that the society's growing dependence on ICT makes it vulnerable to the misuse and disruption of ICT systems. According to the Australian 2009 strategy the aim of the government is to maintain a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy. Confronting and managing risks "must be balanced against […] the need to promote efficiency and innovation to ensure that Australia realises the full potential of the digital economy". More recently, the public discussion paper "Connecting with Confidence" stresses that "Australia's future prosperity is linked increasingly to the confidence and trust businesses and consumers have in [its] digital economy" (Australian Government, 2011). The 2011 UK Cybersecurity Strategy recognises that as the Internet drives economic growth and supports open and strong societies, the cost of cyber incidents for businesses, the potential reduction in trust towards online communications "can now cause serious economic and social harm to the UK" (UK Cabinet Office, 2011a). The 2009 US Cyber Policy Review stresses that the country "faces the dual challenge of maintaining an environment that promotes efficiency, innovation, economic prosperity and free trade while also promoting safety, security, civil liberties and privacy rights. It is the fundamental responsibility of our government to

address strategic vulnerabilities in cyberspace and ensure that the US and the world realise the full potential of the information technology revolution" (US White House, 2009). Japan recognises the need to develop a safe and secure use of ICT to enable the use of ICT to solve the key challenges it faces such as economic growth, ageing society and environmental issues. The aim of the strategy is to "guarantee the nation's safety and security by improving its ability to respond to all types of ICT threats, including cyber attacks, to the world's highest level, […] as well as to build an environment where the nation can actively utilize ICT without concerns regarding information security reliability".

The result is the elevation of this overall subject matter as a government policy priority and a higher degree of governmental co-ordination.

As a result of this context, the overall issue of cybersecurity is elevated amongst government priorities and benefits from more governmental co-ordination. The strategies are generally expressed through one major policy document adopted at a high level of the government, sometimes at the highest (Head of State, Cabinet Office, Prime Minister), sometimes by a ministry acting as the co-ordinator of a process that involved several ministries and agencies across the government. The first objective of most strategies is to improve the organisation of the government to address cybersecurity by assigning clear responsibilities to various government bodies.

In the case of Japan and the United States, the overarching document adopted at the highest level is supplemented by several others addressing specific aspects of the strategy and adopted by agencies or ministries responsible for these aspects. The titles of these documents vary, sometimes reflecting the perspective that each country takes to the problem. The term "strategy" is generally used, although not necessarily in a consistent manner. In some instances, the government carried out a consultation process with the private sector, for example through interviews and workshops (Netherlands) or via the Internet (Australia's Cyber White Paper).

The concepts of "cybersecurity" and "cyberspace" are not used by all countries. However, the scope of most strategies generally covers all information systems and networks, including critical information infrastructures that are not connected to the Internet.

While some countries use concepts like "cybersecurity" and "cyberspace", others continue to use "security of information systems" (France) and "information security" (Japan) or a mix of cybersecurity and "safe and reliable ICT" (Netherlands). Some countries provide definitions of cyberspace and cybersecurity.

The scope of the strategies generally includes all information systems, both connected to the Internet or not, and in particular information systems and networks that support critical infrastructures.[14] As an exception, the German strategy considers that IT systems in an isolated virtual space are not part of cyberspace.

Key concepts

While cybersecurity strategies share common concepts...

Strategies generally lay out a narrative which varies across countries and leads to the introduction of various key objectives and concepts (see Annex IV). Nevertheless, they share the following common concepts:

- Holistic / integrated / comprehensive approach supported by strong leadership

There is a general agreement on the need for a more holistic approach to cybersecurity policy making. Comprehensiveness, in this context, means in general the inclusion of all facets of the problem, such as for example economic, social, educational, legal, law enforcement, technical, diplomatic, military, and intelligence-related aspects, as well as all participants inside the government (see below government co-ordination) and outside, throughout the society (including businesses and individuals) and beyond, with foreign partners.

For example, Australia aims to develop a "government-led coherent, integrated approach" (Australian Government, 2009) and Germany stresses that "cybersecurity must be based on a comprehensive approach" and requires a "high level of government commitment" (Federal Ministry of the Interior, 2011). The US government aims to "integrate competing interests to derive a holistic vision and plan" (US White House, 2009). The United Kingdom supports a "coherent approach to cybersecurity in which the Government, organisations across all sectors, the public and international partners all have a part to play" (United Kingdom). While themes such as the protection of the critical information infrastructure, the fight against cybercrime, the protection of information systems and networks, and others are still relevant and can be identified in the actions outlined in the strategies, they are now blended together in a holistic fashion under a single umbrella which is sometimes tagged with a specific term such as "cyber-security" (Australia, UK) or "cyberdefense"[15] (France). At the EU level, ENISA recognised the need for an integrated approach in 2011[16].

- Government co-ordination

The need for a holistic approach raises the challenge of government co-ordination to enable many government agencies to work together in a coherent manner, avoid duplication, foster synergies and pool initiatives. The scope of government co-ordination is very broad, from the economic and social sectors to the law enforcement, national security, intelligence, military and diplomatic sectors. To address this challenge, strategies assign clear cybersecurity co-ordination responsibilities to existing or new management structures (see below, management structures) at policy and operational levels. In some countries such as Canada, a specific emphasis is placed on the involvement of all layers of government (local, regional/ provincial/territorial, federal).

- Public-Private Partnerships

Most strategies recognise that cyberspace is largely owned and operated by the private sector and that policies should be based on public-private partnerships, which may include business, civil society and the academia. However, they place variable emphasis on this aspect. For example, it might be mentioned as a concept in the strategy (Australia, Canada, Netherlands, UK) or simply reflected in the action plans (*e.g.* France).

Partnering of the federal government with provincial and territorial governments, the private sector, non-governmental organisations and the academia is a key pillar of the Canadian strategy. The UK 2009 Strategy recognises that the success of the National Cyber Security Programme (EUR 777 million over 4 years[17]) depends on the critical role that the private sector has to play and should be based on "a genuine partnership where policy is co-designed so that a credible national response can be delivered" (UK Prime Minister, 2010a). Japan highlights that "the role of public and private sectors must be clearly identified in the course of building an alliance between the two sectors" (Japanese Information Security Policy Council, 2010). The Dutch strategy notes that public-private partnerships should be based on mutual trust, considering both sides as equal partners, enabling gains for every party and following co-operation models with clearly defined tasks, responsibilities, powers and guarantees (Dutch Ministry of Security and Justice, 2011).

- International co-operation

Most strategies also stress the importance of the international dimension of cybersecurity and the need for better alliances and partnerships with like-minded countries or allies, including capacity building of less developed countries. Most countries however provide little detail on how to achieve international objectives, except for the United States which developed a

specific international strategy for cyberspace and the United Kingdom which initiated an international dialogue at the London Conference on Cyberspace in November 2011. The need for a higher degree of harmonisation of legislation against cybercrime is often pointed out, generally in support of the 2001 Budapest Convention on Cybercrime.

Australia promotes an "active international engagement" based on an "active, multilayered approach to international engagement on cyber security" (Australian Government, 2009). Canada stresses international collaboration as essential to secure cyberspace and the benefit from being seen internationally and domestically as a trusted partner in making cyberspace safer. It supports international efforts to develop and implement a global cyber governance regime that will enhance security. The Canadian government plans to develop a cybersecurity foreign policy. The development of international co-operation is one of the main objectives of the French national strategy. Japan stresses that international alliances must be reinforced as "unprecedented borderless incidents are now more likely to occur" (Japanese Information Security Policy Council, 2010). The US International Strategy for Cyberspace in 2011 aims to "unify [its] engagement with international partners on the full range of cyber issues" and provides "the context for [its] partners at home and abroad to understand [its] priorities and how [they] can come together to preserve the character of cyberspace and reduce the threats [they] face" (US White House, 2011a). The United Kingdom takes as a guiding principle the need to favour a multilateral approach (UK Prime Minister, 2009), to seek partnerships with like-minded countries and reach out to others, where possible. The United Kingdom took the lead in a multilateral dialogue with the 2011 London Conference on Cyberspace and promotes the adoption of international norms of behaviour in cyberspace (UK Cabinet Office, 2011a; UK Foreign and Commonwealth Office, 2011). This concept is also supported in the Australian and German strategies.

Most strategies also mention the role of international organisations but they provide little detail as to the role that each organisation plays or should play and how to ensure consistency across them. In general, they mention the Council of Europe, the G8, the Internet Governance Forum, the OECD, the Organisation for Security and Co-operation in Europe (OSCE), and the United Nations. The North Atlantic Treaty Organisation (NATO) is also mentioned by several countries with respect to cybersecurity in the military context (Canada, Finland, Germany, Netherlands, Spain, United Kingdom). The European Union is mentioned by European countries. Spain and Germany indicate a possible extension of the role of the European Network and Information Security Agency (ENISA).

- Fundamental values

Finally, consistent with the Security Guidelines (Democracy principle), most strategies recognise the respect of fundamental values such as freedom of expression, privacy protection and the free flow of information as essential. In addition, Canada stresses the rule of law and accountability as key values. The Dutch strategy calls for proportionate measures based on risk assessment taking into account the balance between the desire for security and the protection of fundamental rights. The UK 2011 strategy stresses that actions to strengthen national security must be consistent with obligations such as freedom of expression, the right to seek, receive and impart ideas, the right to privacy and the commitment to uphold civil liberties. The international norms of behaviour in cyberspace proposed by the UK Foreign Secretary include fundamental values. More generally, the strategy proposes to start from the belief that behaviour which is unacceptable offline should also be unacceptable on line. The planned Australian Cyber White Paper also includes the idea that issues in the online world should be dealt with in a manner consistent with similar issues off line.

… some concepts are specific to some countries, such as the economic aspects of cybersecurity, the need for dynamic policies and the emergence of "sovereignty" considerations.

Countries place a variable emphasis on *economic aspects of cybersecurity* in their strategies: some countries make a reference to information security (and privacy) in their economic growth strategy (Japanese Cabinet Office, 2010),[18] some develop a specific strategic document dedicated to economic aspects (US Department of Commerce, 2011) and others consider economic measures as part of the main actions to be taken by the government (Australia, France, United Kingdom). Interestingly, the UK 2011 strategy aims to enable the promotion of the country as a good place to do business in cyberspace, thus developing a competitive advantage for the country in cyberspace (UK Cabinet Office, 2011a, UK National Security Review, 2010). A similar idea can be found in the Spanish Security Strategy according to which the development of a safe cyberspace can give Spain a competitive edge (*Gobierno de España*, 2011). In some cases, strategies underline the need to maintain or develop technological independence or sovereignty in core strategic IT competences (Germany, Spain).

Some countries recognise the need for *policies tailored to a dynamic environment*, for more rapid, flexible, and agile government cybersecurity policy making and implementation mechanisms. The United Kingdom promotes a "flexible cyber security response" (UK SDSR). Japan supports policies adapted to technical innovation, active rather than passive security

measures, encouraging methodologies such as the Plan-Do-Check-Act cycle approach and other methods that enable to actively implement new measures (Japanese Information Policy Council, 2010). The Netherlands addresses the changing environment by encouraging self-regulation wherever possible, considering legislation only as an alternative when self-regulation does not work[19] (Dutch 2011 Strategy). Canada stresses the need to allow continual improvements to be made to meet emerging threats (Government of Canada, 2010). The 2002 Security Guidelines responded to the challenge of generalised interconnectedness creating an ever changing and instable IT environment by recognising the need for dynamic security concepts (risk assessment, reassessment, shared responsibility, awareness, response, etc.). However, they did not address how to develop and implement dynamic policies to support these concepts. Further, countries are now faced with the need to dynamically manage cybersecurity as a problem of national scale.

The *emergence of "sovereignty" considerations* (*i.e.* national security, intelligence, defence and the military) in the sphere of information systems and networks policy making is probably the most striking consequence of countries considering the interests of society as a whole in addition to each participant separately. While sovereignty considerations and sovereignty government bodies have never been completely absent from the IT sphere,[20] they did not appear specifically in cybersecurity policy making in the past. The new generation of strategies now embed this dimension explicitly. For example, the US DoD strategy is included in the holistic approach adopted by the US Government to address cybersecurity[21] and the US International Strategy for Cyberspace includes a "Defense objective" and a military policy priority (US White House, 2011, p. 12 and 20). The French strategy aims to promote France as a global "cyberdefense" power although the concept of "cyberdefense" in this context is not necessarily related to the military. The UK 2009 strategy briefly discusses this aspect and "recognises the need to develop military and civil capabilities, both nationally and with allies, to ensure we can defend against attack, and take steps against adversaries where necessary". The German strategy also includes the military dimension of cybersecurity but makes a clear distinction with civilian cybersecurity.[22] The emergence of sovereignty considerations in cybersecurity policy making is reinforced by the fact that related government agencies play a role both in the cybersecurity policy making process as well as at the operational level (see below).

The strategies are consistent with the principles of the 2002 OECD Security Guidelines but they do not mention them. Nevertheless, they introduce the concept of business continuity (or resilience) and real time management which are not as such in the Guidelines …

The 2002 Security Guidelines provided nine principles to create a general frame of reference for participants to understand security issues and respect ethical values in the development and implementation of coherent policies for the security of information systems and networks. Although national strategies never mention the OECD Security Guidelines, they all reflect their principles.

In addition, many strategies highlight "resilience" of information systems and networks as a key strategic concept which is absent from the Security Guidelines. Resilience, which is however not precisely defined in the strategies, can be understood as the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.[23] It is more generally related to the concept of business continuity. It appears as the response to the recognition that some level of risk has to be accepted which implies that some incidents will occur and some attacks will reach their objective. As such, it is consistent with the Guidelines which introduced risk management as a fundamental approach for the security of information systems and networks. Resilience is related to several principles of the Security Guidelines, such as Response (3), Risk Assessment (6), Security Design and Implementation (7) and Security Management (8). Similarly, while the Security Guidelines focus on timeliness of Response, action plans introduced with several strategies emphasise the need for real time operational management based on situational awareness (see below).

Management structures and actions plans

Most strategies include plans that identify organisational decisions and priority actions, generally described at a high level of generality. Sometimes, the main strategic documents are associated with more detailed action plans. This report does not review the details of all action plans but rather focuses on their main characteristics, in particular as compared to previous policy packages.

All strategies establish stronger government co-ordination mechanisms and most highlight leadership as a key factor. However, there is no universal approach regarding how governments organise themselves to address these issues.

Most strategies aim to improve the public administration's organisation and co-ordination to address cybersecurity. Almost all strategies assign clearer responsibilities in the government and/or establish new organisational structures. Some place a strong emphasis on the need for high-level leadership. While all countries target the same objectives, the organisational arrangements they make vary and reflect their cultures and styles of government. In general, however, strategies place a strong emphasis on the identification of a co-ordination point at the policy level and at the operational level. Policy coordination can be assigned to Prime Minister, Cabinet office (Australia, Japan, United Kingdom), or Head of State (*e.g.* "Cybersecurity Czar" reporting to the White House), to a specific agency for cybersecurity attached to a co-ordination body (*e.g.* the French ANSSI) or to a Ministry (Canada, Germany, Netherlands). Co-ordination at operational level generally relies on a central point which varies considerably across countries. Some countries also created a specific body for public-private co-ordination and to provide advice to the government regarding how to balance cybersecurity, economic objectives and fundamental values (*e.g.* Dutch and German National Cyber Security Councils).

For example,

- In Australia, policy development is led by the **Cyber Policy Coordinator/National Chief Information Officer** within the Department of the Prime Minister and Cabine,t[24] under the National Security Advisor. A guiding principle is that the scale and complexity of the cybersecurity challenge requires strong national leadership from a number of agencies including the Attorney-General's Department, which chairs the **Cyber Security Policy Committee**[25] on which operational agencies are represented. At operational level, the 2009 Cybersecurity strategy established a new government CERT (CERT Australia) and the Australian Defence White Paper created the Cyber Security Operation Center (CSOC) to provide the government with all-source cyber situational awareness and an enhanced ability to facilitate operational responses to events of national importance.
- Public Safety Canada is responsible for the co-ordination of the implementation of the Canadian strategy and for designing an approach to reporting on this implementation. It is also in charge of public cybersecurity awareness. Within Public Safety Canada, the

Canadian Cyber Incident Response Centre monitors the cyber threat environment, provides mitigation advice on cyber threats and co-ordinates the national response to cyber security incidents, focusing on critical infrastructures. Several other agencies are involved, including Industry Canada as regards the digital economy strategy to create a safer and trusted online marketplace, Treasury Board Secretariat for government cybersecurity, intelligence and cryptography agencies, the Department of Justice with respect to cybersecurity legislation, Foreign Affairs and International Trade Canada in relation to the international dimension of cybersecurity. The Department of National Defense and the Canadian Forces are involved as regards the security of their own networks, information sharing with other departments and relationships with foreign military allies.

- In Finland, while the government has not yet adopted a comprehensive cybersecurity strategy, it has nevertheless assigned responsibility to the Ministry of Finance's Government Information Security Management Board (VAHTI) for co-ordination with respect to cybersecurity within the government.

- France created a national authority for the security of information systems, the **National Agency for the Security of Information Systems** (ANSSI), attached to the Secretary General of Defense and National Security (SGDSN) who reports to the Prime Minister.[26] ANSSI is an interagency coordinator of governmental action and its missions include providing secure interagency means of communications, inspecting government systems, acting as a government CERT, providing certification for systems protecting state secrets, acting as an international point of contact and providing training.[27]

- The development of the German strategy was led by the Federal Ministry of the Interior in co-operation with other ministries and in particular the Foreign Office and Ministries of Defence, Economics and Justice. According to the strategy, the government has established a **National Cyber Response Centre** to optimise operational co-operation within the government and co-ordination of protection and response measures to IT incidents. The Federal Office for Information Security (BSI) is responsible for the Centre. Other authorities like the Federal Office for the Protection of the Constitution (BfV) and Federal Office of Civil Protection and Disaster Assistance (BKK), the Federal Criminal Police Office (BKA), the Federal Police (BPOL), the Customs Criminological Office (ZKA), the Federal Intelligence Service (BND), the military (Bundeswehr) and authorities supervising critical infrastructure operators are co-operating directly with each

other in this centre within the framework of their statutory tasks and power. The Centre will inform directly the Federal Ministry of the Interior in case of a crisis. In addition, a **National Cyber Security Council** has been established to strengthen cooperation within the government and with the private sector and provide recommendations at high political levels on strategic issues. The Council is under the responsibility of the Federal Government Commissioner for Information Technology (BfIT) and comprises representatives from the Federal Chancellery and State Secretaries from the Foreign Office, Ministries of the Interior, Defence, Economics and Technology, Justice, Finance, Education and Research, and representatives from the federal Länder (regions). It also includes representatives from business as associated members and the academia, as appropriate. The National Cyber Response Centre will submit recommendations to the National Cyber Security Council.

- Japan places some focus on the need to "establish an organisational systems to implement a comprehensive policy under strong leadership through an alliance of the concerned government agencies centred around the Cabinet Secretariat".

- The Dutch government assigned co-ordination and coherence responsibility to the Ministry of Security and Justice and promotes a network-centred form of collaboration. It created a **National Cyber Security Center** with a strategic and implementation responsibility, incorporating the current GOVCERT.NL, to provide expertise and advice, support and execute response during incidents, enhance crisis management. The Center is responsible for threat and risk analysis, creating a single comprehensive picture of the current ICT threat. It also includes the ICT Response Board, a public-private partnership that gives advice on how to counteract major ICT disruptions to decision-making organisations. It also created a **National Cyber Security Council** with representatives from public and private sectors as well as the academia to help improve the understanding of cyber security developments and help parties deal with incidents and make decisions in crisis. The Council is co-chaired by public and private representatives.

- The UK established an Office of Cyber Security (OCS) subsequently renamed **Office of Cyber Security and Information Assurance** (OCSIA) in the Cabinet Office[28] to provide strategic leadership for and coherence across the government. OCSIA delivered the cyber-security strategy. Its missions include providing strategic direction, supporting education, awareness and training, working with the

private sector, working with the Office of the Government Chief Information Office (OGCIO) to ensure resilience and security of government infrastructures, engaging with international partners. The 2009 Cyber Security Strategy also created a **Cyber Security Operations Centre** (CSOC) to actively monitor the health of cyberspace, provide collective situational awareness, enable better understanding of attacks against UK networks and users, co-ordinate incident response and provide better advice and information about the risks to business and the public. It is a multi-agency body hosted by Government Communications Headquarters (GCHQ) in Cheltenham, alongside GCHQ's Information Assurance arm, Communications Electronics Security Group (CESG).

- The US Cyber Policy Review focused on the lack of organisation of its administration and on improving the distribution of responsibilities for cybersecurity and decision authority to direct action across the government. Cybersecurity was designated as one of the President's key management priorities. A **cybersecurity co-ordinator** was appointed and the Cybersecurity Office was created within the National Security Staff at the White House, working closely with the Federal Chief Information Officer and the National Economic Council. The Cyber Policy review included several organisational actions, such as the designation of a privacy and civil liberties official to the National Security Council Cybersecurity Directorate and the establishment of a formal interagency process.

"Sovereignty agencies" play an operational role for cybersecurity in most countries.

Among the various agencies involved in their implementation, most strategies assign an operational role to agencies with sovereignty responsibility such as ministries of defence and agencies in charge of intelligence and other "national security" missions. These include agencies in charge of cryptography expertise (*e.g.* Communications Security Establishment Canada), civilian and/or military intelligence services (*e.g.* Canadian Security Intelligence Service, Dutch General Intelligence and Security Service (AIVD) and Military Intelligence and Security Service (MIVD), the UK GCHQ. The Dutch strategy recognises the need to prioritise co-operation throughout the entire system between civilian and military parties. In the 2011 UK strategy, the overall budget for the four-year National Cyber Security Programme includes shares for the Signal Intelligence Account and Ministry of Defence which are recognised, in the strategy, as having a strong role in improving the understanding of and reducing the vulnerabilities and threats the country faces in cyberspace.

Cybersecurity strategies strengthen priorities identified in 2003-2004 …

All strategies reinforce areas of priority that were defined in the first generation of strategies for the security of information systems and networks (see OECD, 2005).

- Enhancing government security and protecting Critical Information Infrastructures (CII)

These two areas highlighted in 2004 as key drivers supporting the development of a culture of security are generally reinforced in 2012. Overall, emerging themes are the need for better organisation and response capability.

All countries include a large range of new measures for better securing government systems, ranging from fostering the use of cryptography and ensuring autonomy in this area, to rationalising government networks, improving the resilience of government systems, developing labelling schemes, promoting strong authentication for civil servants, developing attack detection/prevention capacity, multiplying Chief Information Security Officers, promoting standards and the use of audit, requiring business continuity plans, establishing procurement requirements, raising awareness of civil servants and developing viable career paths for security experts, etc. Most countries also have created or are creating a government CSIRT. Where it already existed, it is strengthened or better resourced. Some countries highlight the importance of co-ordinating the various layers of governments (Canada and Germany). The UK stresses the importance of cybersecurity in the context of its Government Cloud Strategy (UK Cabinet Office, 2011a and 2011b). In many cases, countries consider the protection of government systems and networks as part of the protection of critical infrastructures.

The protection of CII is generally part of the cybersecurity strategies although countries generally have specific policy documents to address this challenge. Some strategies stress the need to better integrate CII management structures with other cybersecurity structures as an objective (Netherlands). Measures for the protection of CII vary depending on the level of advancement of each country in that area and are generally based on public-private co-operation. They include preparatory measures such as cybersecurity incident response plans and improved crisis management plans, the development of business continuity arrangements, the organisation of exercises, the creation of a rapid response capacity with international reach, the improved co-ordination of and information sharing amongst the various players (*e.g.* suppliers and operators of CI, public and private actors, etc.), the development of legal frameworks, international alliances, the promotion of standards and the organisation of audits.

- Enhancing the fight against cybercrime

As regards cybercrime, most countries focus their efforts on the development of their law enforcement capacity. Some countries highlight the need to improve their legal framework (Canada, France, Japan, United Kingdom), to reinforce international co-operation (France, Germany, Japan) and regionally harmonise criminal law (Spain). The United Kingdom developed a dedicated cybercrime strategy in 2010 which describes the current cybercrime situation, provides a vision, and details how the government will achieve its objectives (UK Home Office, 2010).[29] Cybersecurity strategies include various measures such as strengthening existing high-tech crime units, training law enforcement staff, involving non-law enforcement experts in police cyber investigations (*e.g.* voluntary "police specials") (UK), creating a pool of registered experts and create cybercrime police knowledge centre, encouraging more cross-border investigation, increasing the number of cybercrime specialists in the judicial system and setting up a police knowledge centre (Netherlands). Canada will establish a centralised Cyber Crime Fusion Centre to respond to requests from the Cyber Incident Response Centre regarding cyber attacks against Government or Canada's critical infrastructure (Government of Canada, 2010). Germany will create a joint institution with industry and law enforcement agencies to exchange know-how (Federal Ministry of the Interior, 2011). Most countries support the Budapest Convention on Cybercrime and some indicate possible examination of the need for further international legislation in his area (Germany, Netherlands).

- Raising awareness and improving education

Awareness raising and education were reported as strong areas of activity in 2004 and are still very important in current strategies. *Awareness raising* initiatives generally focus on the general population, including specific targets such as children (Australia, Spain, United Kingdom), and on businesses and government bodies, including specific targets such as decision makers, and critical infrastructures. Education efforts towards the general population include, for example, cyber hygiene education in schools at all levels (Netherlands), using social media (United Kingdom), through partnerships with ISPs (see below), via the possible establishment of an "information security support service" (Japan). The United Kingdom supports the development of market differentiators, including certified safety labels for products and services, and industry-led standards and guidance. The Netherlands established a cyber security education and training centre. Australia supports the concept of responsible digital citizenship based on digital literacy and awareness to exploit online opportunities and effectively mitigate cyber risks.

In contrast with 2004, the *lack of a cybersecurity workforce* is identified as a key policy challenge by governments. The United States, for example, compares the situation with the effort to upgrade science and mathematics education in the 1950s. The UK strategy recognises the need to better understand the demand for cyber security skills across the private sector. Several countries promote the development of viable career paths. The United Kingdom aims to encourage the development of a community of "ethical hackers". Measures include, for example, establishing programmes of certified specialist training (Netherlands, United Kingdom), supporting a Cyber Security Challenge[30], strengthening postgraduate education and developing a coherent cross-sector research agenda to strengthen the academic base (United Kingdom).

- Research and Development

Research and Development which was identified as an area of lower attention in 2004 is featured prominently in current strategies. Countries support a public-private approach to R&D and aim to better co-ordinate research efforts which used to be fragmented. The most significant effort is the publication by the US White House in December 2011 of its Strategic Plan for Federal Cybersecurity Research and Development Program. The strategy aims to induce change by understanding the root causes of cybersecurity deficiencies rather than just addressing symptoms, develop scientific foundations for security by stimulating research in areas such as biology, economics and other social sciences, maximise research impact through co-ordination and collaboration of agencies across the government and accelerate transition to practice.

… and introduce new themes.

- **Develop a "situational awareness" capacity**: all strategies aim to enhance their ability to collect real-time information about online threats. Real-time monitoring capability is sometimes joined with response capacity through the creation of operation rooms of various kinds. This aspect of the strategies is sometimes related to the development of a cyber intelligence capability.
- **Develop an industrial policy for cybersecurity** (France, United Kingdom, United States). For example, France aims to support innovative SMEs in the security sector. The US DoD "will promote opportunities for SMEs and work with entrepreneurs in Silicon Valley and other US technology innovation hubs […]". Several strategies include leveraging public procurement to help cyber security SMEs. The UK 2011 strategy calls for exploring how GCHQ's expertise can more directly benefit economic growth and

support the development of the UK cyber security sector without compromising its mission. Initiatives could include commercial exploitation of GCHQ expertise, partnerships with various players to foster cybersecurity innovation, and government-sponsored venture capital model to unlock cybersecurity innovation in SMEs. Spain highlights the need to support the development of private national companies in this strategic sector "where reliance on foreign firms could be dangerous".

- **Specifically address key business players or sectors**: the United Kingdom and the United States call for specific measures to better protect businesses that are not part of the national critical infrastructure but which nevertheless represent important economic assets for the country.

– The United States developed the concept of an "Internet and Information Innovation Sector (I3S)" which includes functions and services that create or utilise the Internet or networking services and have large potential for growth, entrepreneurship and vitalization of the economy but would fall outside of CI as defined by the government (US Department of Commerce, 2011). A nationally recognised approach would be developed to minimise vulnerabilities in this sector, including through the development of codes of conduct, promotion of standards, of automation in security and through improved security assurance. Incentives would be leveraged to help I3S combat cyber threats, call for education and research and international co-operation.

– The United Kingdom established a "cybersecurity hub" gathering largest companies from all sectors where the threat to revenues and intellectual property is capable of causing significant economic damage to the United Kingdom. This public/private hub aims to facilitate the exchange of actionable information on threats and strengthen response to incidents, analyse new trends, and work to strengthen collective cybersecurity capabilities (UK Cabinet Office, 2011a, 4.20). In another initiative, the British government addresses specifically the retail sector through the creation of a Retail Cyber Security Forum to establish effective reporting and information sharing.[31]

– Germany created a task force to address specifically IT security in small and medium-sized businesses (German Federal Ministry of the Interior, 2011).

- **Foster partnerships with Internet Service Providers (ISPs)**: where, for example, ISPs inform their customers when their equipment is identified as taking part in a botnet and take action to assist them in solving the problem. Such initiatives are emphasised by Australia, Japan, the United Kingdom, and the United States. These initiatives have been studied elsewhere by the OECD (OECD, 2012a). Germany, which also adopted a similar initiative, stresses the possibility for providers to assume greater responsibility including making available to users a basic collection of appropriate security products and services (German Federal Ministry of the Interior, 2011).

- **Identify economic drivers and incentives** to improve business response, for example through insurance or liability frameworks is highlighted by the United Kingdom and the United States. Initiatives include the development of market differentiators such as certified cyber security labels (see above) and the possibility to develop a cyber insurance market (US Department of Commerce, 2011). The UK Department for Business, Innovation and Skills (BIS) will hold a strategic summit with professional business services providers including insurers, lawyers and auditors to discuss how they can develop the services they offer to business to help them manage and reduce risks.[32] Several countries support the mandatory notification of breach of personal data and reporting mechanisms for data leakages in critical sectors (*e.g.* telecommunications).

- **Develop digital identity frameworks**: Spain is rolling out electronic identification documents to its population through an ambitious digital identity plan. The development of a strategy to foster stronger digital identity is part of the US strategic package (US White House, 2011b. See also OECD, 2011) and was mentioned by Japan in relation to the improvement of its identity number scheme.[33] France plans to roll out an electronic card enabling strong authentication for civil servants. The Dutch strategy mentions the consideration of an electronic identity card with electronic authentication and signature features. The German strategy stresses the provision of basic security functions by the state, such as electronic proof of identity or certified e-mail[34] (German Federal Ministry of the Interior, 2011). The UK National Cyber Security Programme includes funding for the development of a trusted and resilient approach to identity assurance (UK Cabinet Office, 2011a, 4.18).

- **Protect children online** (Australia and Spain).
- **Carry out cyber security exercises** to enhance incident response co-ordination, including across borders (Japan, Netherlands, Spain, and United States)
- Address concerns related to the **security of supply chains** (Canada, Unites States).
- **Develop a cyberdefense military capacity**: the protection of military networks and the development of an offensive cyber capacity is mentioned by some cybersecurity strategies but without much detail (France, United Kingdom, United States). The German strategy makes a clear distinction between civilian and military cybersecurity which focus respectively on IT systems in use in the civilian and military German cyberspace.

All countries support the establishment of stronger international mechanisms.

International co-operation was considered as important in 2004 but limited to the sharing of best practices and guidance. All countries' strategies now emphasise the need to reinforce international co-operation. International co-operation results from the inherently transnational nature of the Internet and some strategies recognise that they rely on partnerships with third countries for some aspects and express willingness to assist foreign partners where possible. Regional co-operation is emphasised by European countries. The need for stronger international efforts is highlighted regarding various aspects:

- Building/reinforcing alliances (United Kingdom, France).
- Participating in discussions carried out in international and regional organisations (see Annex I).
- Developing internationally recognised norms of behaviour for cyberspace (Australia, United Kingdom) or a code for state conduct in cyberspace (Germany), including confidence building measures.
- Initiating and/or participating in multilateral discussions, such as the UK Conference on Cyberspace in London on 1-2 November 2011.
- Encouraging third countries to join the 2001 Budapest Convention (Netherlands) and/or to adopt laws compatible with the Convention (UK). Ratifying the Convention (Canada).
- Organising/participating in international cybersecurity exercises.

- Developing a capacity to assist other countries in case of crisis (France) and help them to build the components of a cybersecurity framework (Japan, United Kingdom, United States).

In several instances, the international dimension of strategies addresses problems which extend beyond the economic and social impact of cyberspace such as the prevention of armed conflict, through, for example, confidence-building measures.

Considerations highlighted by non-governmental stakeholders

This section introduces some of the considerations and suggestions expressed by the business, civil society, and the Internet technical community in their response to a questionnaire circulated in January 2011 (cf. Annex VI and OECD, 2012b).

While non-governmental stakeholders' responses reflect variations as regards priority areas of concern, they exhibit the following strong points of convergence: *i)* multistakeholder collaboration and co-operation are the best means to develop effective cybersecurity policy that respects the fundamentally global, open and interoperable nature of the Internet; *ii)* policy options must be flexible enough to accommodate the dynamic nature of the Internet; *iii)* more robust evidence-based cybersecurity policy making is needed, an area which is generally not covered by cybersecurity strategies.

Non-governmental stakeholders share some concerns with respect to **the emergence of sovereignty considerations** in cybersecurity and stress the importance of enhanced multistakeholder dialogue to overcome these challenges.

Business recognises that the divide between national security and economic security is increasingly blurred, in particular as more critical infrastructures are owned by the private sector. It stresses that in exercising their sovereignty competencies, governments may adopt cybersecurity policies which impact economic security and private sector systems as well as create burdens on business. Greater emphasis on enhanced consultation and co-operation with business could help governments find the appropriate balance between sovereignty and economic and social cybersecurity.

Civil society also recognises this increasingly blurred divide and is concerned that the emergence of sovereignty considerations in cybersecurity reduces its participation in the policy making process. This could for example result from the involvement and lobbying of the security industry and law enforcement, opaque policy processes, strong military and intelligence interests, public-private partnerships modelled on traditional intelligence

communities rather than Internet governance ones, and finally state-to-state interactions taking place in closed settings. Another concern is that the lack of specificity of the term "cybersecurity" in conjunction with the emergence of sovereignty considerations in cybersecurity policy making may lead to re-couch all cybersecurity issues into the language of "national security" and warfare, preventing balanced policy making and fostering the adoption of drastic solutions such as network monitoring instead of other practical solutions more respectful of citizens' rights. Discussions related to the protection of critical information infrastructures might influence broader cybersecurity debates towards national security thereby justifying sweeping unaccountable powers. Finally, the extension of state rivalries in cyberspace is pointed out by civil society as creating one of the chief security threats on line, for example by increasing the market demand for exploits and threats which can proliferate into the civilian economy.

To limit possible challenges raised by the blurred divide between sovereignty and economic and social considerations, the civil society suggests that policy initiatives target specific and narrowly defined tangible and demonstrable harms in order to prevent an overarching security blanket which would suffocate the very society it seeks to protect. This suggestion could enable better informed decision making and balancing of the expected security benefits with the possible impact on fundamental rights. It could be viewed as a proposed "Transparency" principle for cybersecurity policy making, building on the risk approach called for in the Security Guidelines (see OECD, 2012b). The civil society also proposes that the impact on fundamental rights of each cybersecurity initiative be assessed so as to enable more informed discussions. It also suggests the adoption of a sunset clause for cybersecurity strategies to avoid policies proportionate to the risks when initially adopted ultimately threatening fundamental rights as technology evolves. Such a measure would also ensure that strategies are reviewed regularly.

Recognising that the protection of children on line is a very important shared objective, the Internet technical community stresses that it should not be misused as a justification for cybersecurity measures that are contrary to an open Internet.

The civil society highlights that legal provisions to enhance cybersecurity can in some countries interfere with legitimate cybersecurity research and deter further R&D and investments in this area. It proposes that an assessment of the consistency of cybersecurity measures would help prevent such counter-productive situations. The civil society also encourages fact-based decision making as a central element of the cybersecurity discussion, while recognising that transparency of risk-related data raises real challenges for the private sector, which faces many disincentives to reveal this type of information, as well as for national security agencies which do not generally operate in full transparency

mode. To cope with these challenges, it suggests that governments disclose metrics regarding risks faced by their own systems and networks rather than relying on external sources of information sometimes linked to the cybersecurity industry. Breach notification requirements put forward by several strategies are mentioned as another source of data. The Internet technical community highlights the need to develop a standard, unified and privacy-respecting method to collect, analyse and report data breaches at the global level in order to provide industry and governments with a better understanding of cybersecurity threats. Data could also result from other measures such as the guidance adopted by the US Securities and Exchange Commission in 2011 regarding disclosure obligations relating to cybersecurity risks and cyber incidents.

The need to address the **international dimension of cybersecurity in relation to trade and innovation** is a key concern for the Internet technical community and for business. The Internet technical community expressed the view that approaches that increase technical barriers to trade in ICT infrastructure equipment and end user devices risk balkanising the Internet into different markets with different technical regulation. Such approaches would reduce economies of scale which have enabled the rapid deployment of broadband infrastructures globally, and could create interoperability issues and harm the growth of global ICTs and other services. For businesses, which often operate globally and face a variety of specific approaches to both economic and sovereignty cybersecurity, coherence of cybersecurity policies at international level is essential. Although differences between national cybersecurity approaches are inevitable, they should allow for the deployment of global cost-effective industry solutions. Thus unilateral requirements to use local standards or technologies, unnecessary or redundant documentation or certifications requirements, as well as interferences in the global value chain create complex challenges. The adoption by third countries of specific requirements may intentionally or inadvertently compromise overall cybersecurity; it can also severely increase cost, limit functionality and constrain innovation, as well as impair trade or skew a level playing field by hindering the ability of companies and organisations to roll out globally consistent processes and infrastructures. Business calls for the adoption of a system of generalised mutual recognition to overcome these difficulties. It also encourages the exploration of cross compliance recognition mechanisms whereby a system which has been found compliant for one set of requirements under one regulation should be recognised as compliant with similar requirements under another regulation. Finally, it calls for governments to promote the use of internationally recognised standards to address this challenge and underlines the role of the OECD to raise the awareness of less developed countries on this issue as well as to lead by example.

The **role of international standards** is emphasised by the Internet technical community which highlights that governments should foster the development of open standards and permission-less innovation for security solutions. This community emphasises the need to respect the well-established channels for Internet standards development (*e.g.* IETF and W3C) and to avoid unilateral modifications to global Internet standards as well as overly prescriptive approaches which risk freezing security solutions and stifling innovation in technology and Internet use. The translation of cybersecurity policy priorities into the technological sphere should support and promote the fundamental principles of the Internet. This community also highlights that the overall objective of a more secure Internet is supported by the development of a variety of technical building blocks through an open, collaborative and consensus-based standards development model.[35] Voluntary security initiatives can also play a role, such as the Software Assurance Forum for Excellence in Code (SAFECode) which focuses on effective software assurance methods, and the Open Group Trusted Technology Forum (OTTF)[36] which focuses on open standards for a more trusted global supply chain.

The Internet technical community underlines its role as a source of independent advice regarding the potential intended and unintended consequences of planned policy decisions on the Internet and the way it functions, and stresses that policy makers should seek such advice as early as possible in the policy development process in order to avoid pursuing technologically flawed decisions.

Finally, the Internet technical community stresses the critical role of the government to provide leadership and co-ordination of cybersecurity efforts through appropriate legal reforms and public-private partnerships to facilitate information sharing and voluntary adoption of best practices by the industry. Multi-stakeholder co-operation and government leadership should aim to ensure functionality of infrastructure and services before, during and after attacks, the development of more robust systems and networks and more secure solutions that preserve the principles of the open Internet. The Internet technical community notes, with the civil society, that governments can play a lead role in the implementation of best practices, including policies, technologies and even legislative requirements to secure their own information systems and networks. The development of well-designed, balanced and judiciously applied trust compliance programmes and procurement practices by governments would provide a clear direction to other economic and social actors. Moreover, government cybersecurity information and experience could in turn benefit the rest of society if it is shared.

Other considerations

The introduction of **sovereignty considerations** in cybersecurity is a turning point that is likely to influence cybersecurity policy making in the longer term and will deserve continued attention and further analysis in the future. As reflected in current strategies, however, most of these sovereignty considerations are generally separated from economic and social aspects of cybersecurity, and are mentioned mainly as a result of the holistic nature of these strategies. For example, strategies stress the protection of military ICT infrastructures as a military matter and mention the responsibility of a relevant government agency, generally the ministry or department of defense. In many cases, the relationship between the economic and social aspects addressed in the strategies and such sovereignty considerations are only mentioned to make a link between government cybersecurity and sharing of information with intelligence agencies.

Nevertheless, some intersections between sovereignty and economic and social aspects of cybersecurity appear in some strategies and in current public cybersecurity policy debates. For example, in some countries, the co-ordination of cybersecurity policy making is taking place in a "national security" co-ordination agency or body such as a National Security Council, or National Security Advisor. Other potential intersections may result from increased sovereignty cybersecurity spending spilling over into the civilian cybersecurity market. For example, the British strategy calls for exploring how the expertise of one of its intelligence agencies can more directly benefit the development of a British cybersecurity industry sector without compromising its mission. Cybersecurity investments driven by defence contracts could change the dynamic of the civilian market, new key players from the defence and security industry[37] could gain more weight in a growing civilian cybersecurity market, introducing innovative products and services as well as a different ethos; cybersecurity personnel hired and trained in the defense forces could several years later enter the civilian cybersecurity jobs market. These possible evolutions could partially address the objectives of several strategies to develop a stronger cybersecurity industry based on enhanced skills and a larger workforce. These examples suggest that the breadth of the grey area where sovereignty and economic and social cybersecurity considerations overlap varies across countries, raising new opportunities and challenges. As cyber-security policy develops, the intersections between the sovereignty and economic and social facets of cybersecurity would need to be carefully analysed, for example to assess their impact on the openness of the Internet, on the supply and demand of cybersecurity products, services, skills and jobs, on fundamental values such as privacy and freedom of speech (Democracy Principle of the Security Guidelines) as well as on the complexity of inter-national co-operation in cybersecurity.

The development of **evidence-based policy making** through appropriate indicators, whether statistical or anecdotal, quantitative or qualitative, is generally absent from the cybersecurity strategies compared in this report. However, it may be considered essential to a risk-based approach at all levels, for better cybersecurity policies and implementation, and for the development of a stronger cybersecurity market.

Although the protection of critical information infrastructures is generally included in the scope of cybersecurity strategies, the issue of **cross-border interdependencies** is rarely addressed at strategic level. Further co-operation on this matter which is addressed in the OECD Recommendation on Protection of Critical Information Infrastructures (2008) would be of mutual interest.

Most strategies mention the need to improve **international co-operation** at policy and operational levels. However, in each country, different organisational arrangements reflecting national cultures and styles of government determine which agency is competent and where co-ordination is taking place. In case of a cross-border crisis where real time co-operation would make a key difference, such differences may become a serious obstacle to smooth collaboration. Nevertheless, the trend towards the establishment of co-ordination mechanisms within governments in order to support more holistic strategies provides an interesting opportunity for each country to establish an official single point of contact for international cybersecurity co-ordination/ co-operation. Such points of contacts could be useful in case of cross-border crisis or for initiating co-operation at various levels on a more regular basis. This would follow-up on the OECD 2008 Recommendation on the Protection of Critical Information Infrastructures which called for governments to "make available information regarding the national agencies involved in the protection of CII, their roles and responsibilities, to facilitate identification of counterparts and improve the timeliness of cross border action".

Finally, several strategies underline the importance of **cyber security exercises** but few take into account the need to develop contingency and response plans in advance as well as the importance of regional and international exercises.

Annex I
Intergovernmental organisations and initiatives

This annex provides a brief overview of intergovernmental bodies and initiatives currently addressing cybersecurity at the policy level[38].

Intergovernmental organisations

- Asia-Pacific Economic Cooperation (APEC)

APEC[39] is a regional economic forum which groups 21 economies to promote free and open trade and investment, regional economic integration, economic and technical co-operation, human security, and a favourable and sustainable business environment to support sustainable economic growth and prosperity in the Asia-Pacific region. Eight APEC members are also OECD members. Its Telecommunications and Information Working Group (APEC TEL) aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing and implementing appropriate telecommunications and information policies. APEC TEL Security and Prosperity Steering Group (SPSG) carries out many activities related to security, trust and confidence in network/infrastructure/services/technologies/applications/e-commerce. Since 2005, OECD co-operates closely with SPSG in various areas such as security of information systems and networks, awareness raising, malware, the protection of children on line and botnets. OECD has "guest status" in APEC TEL. APEC TEL meets twice a year and organises regularly APEC Telecommunications and Information Industry Ministers' Meetings (TELMIN).

- Council of Europe

The Council of Europe helps protect societies worldwide from the threat of cybercrime through the Budapest Convention on Cybercrime, the Cybercrime Convention Committee (T-CY) and the technical co-operation Programme on Cybercrime. The Budapest Convention on Cybercrime was adopted on 8 November 2001 as the first international treaty addressing crimes committed using or against network and information systems (computers). It entered into force on 1 July 2004. As of April 2012, 28 OECD

members had signed the Convention and 17 had ratified it. A total of 32 countries had ratified/accesses to the Budapest Convention,[40] which is open for ratification/accession by countries which are not members of the Council of Europe. The Convention foresees regular consultations of the Parties who meet at least once per year as the Cybercrime Convention Committee (T-CY). The OECD is an observer in the T-CY and the Council of Europe is an observer in the OECD Working Party on Information Security and Privacy. The Council of Europe also helps countries to ratify, accede and implement these treaties through technical co-operation projects. It carried out over 250 activities through its Global Project on Cybercrime since 2006 as well as the regional joint projects of the European Union and the Council of Europe on cybercrime (CyberCrime@IPA and Cybercrime@EAP). The Council of Europe organises every year the Octopus Conference on Co-operation on Cybercrime in Strasbourg, France.[41]

- European Union

See Annex II.

- G8

The involvement of the **G8** in the field of cybercrime dates back to the late 90s, when the G8 created a mechanism to expedite contacts between countries, the so-called "G8 24/7 network of contact points". In May 2003, the G8 adopted the G8 Principles for Protecting Critical Information Infrastructures on the fight against crimes and terrorist acts committed using or against network and information systems ("cyber-crime" and "cyber-terrorism"). In May 2004 the G8 Justice and Home Affairs Ministers adopted the Best Practices for Network Security, Incident Response and Reporting to Law Enforcement and in May 2009 a significant part of the Final Declaration was devoted to cybercrime and cybersecurity, focusing on collaboration between service providers and law enforcement and on the strengthening of international co-operation. Internet was among the key priorities of the G8 2011 Deauville Summit which was preceded by an "e-G8" event held in Paris prior to the Summit. G8 Leaders agreed on a "number of key principles, including freedom, respect for privacy and intellectual property, multi-stakeholder governance, cyber-security, and protection from crime, that underpin a strong and flourishing Internet".[42]

- Internet Governance Forum (IGF)

The IGF was established by the World Summit on the Information Society in 2006 to bring people together from various stakeholder groups in discussions on public policy issues relating to the Internet. While there is no negotiated outcome, the IGF informs and inspires those with policy making power in both the public and private sectors. The IGF facilitates a common

understanding of how to maximise Internet opportunities and address risks and challenges. It is convened under the auspices of the Secretary-General of the United Nations. Its mandate includes the discussion of public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet. Themes related to cybersecurity are regularly discussed in the annual IGF meeting and in regional IGF type settings.[43]

- North Atlantic Treaty Organisation (NATO)

NATO has recently acknowledged the need to focus on cyber defence. In the 2010 Strategic Concept adopted in Lisbon, NATO Allies recognised the need for NATO to develop further the ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and co-ordinate national cyber-defence capabilities, bringing all NATO bodies under centralised cyber protection, and better integrating NATO cyber awareness, warning and response with member nations. The Cooperative Cyber Defence Centre of Excellence (CCD-COE)[44] was created in 2006 in Tallinn, Estonia. It is an international military organisation whose mission is to enhance the capability, co-operation and information sharing among NATO, NATO nations and Partners in cyber defence by virtue of education, research and development, lessons learned and consultation.

- Organisation for Economic Co-operation and Development (OECD)

Within the broader objective of the OECD to develop "better policies for better lives", the OECD Committee for Information, Computer and Communications Policy (ICCP) promotes Internet policies that unleash innovation and capture new sources of growth for more inclusive economic development and increased social well-being. Its Working Party on Information Security and Privacy (WPISP**)** develops flexible policy recommendations and guidance to sustain trust in the Internet Economy and the global networked society. Its work is based on in-depth policy analysis in areas such as National Cybersecurity Policies, Indicators for cybersecurity and privacy, Critical Information Infrastructure Protection (CIIP), digital identity management, malware, Radio-Frequency Identification (RFID), privacy protection and the protection of children online. WPISP Participants are delegates from 34 OECD member countries, observers, other international organisations as well as representatives of business, civil society and the Internet Technical Community.

- Organisation for Security and Cooperation in Europe (OSCE)

The OSCE addresses a wide range of security-related concerns, including arms control, confidence- and security-building measures, human rights, national minorities, democratisation, policing strategies, counter-terrorism and economic and environmental activities. Enhancing cyber security has become a cross-dimensional topic and endeavour in the OSCE. OSCE has carried out a number of cyber-security events since 2005, the last of which focused on its future role in tackling challenges arising from cyberspace (9-10 May 2011).[45]

- Organisation of American States (OAS)

The OAS groups 35 independent states of the Americas which adopted in 2004 a Comprehensive American Strategy to Combat Threats to Cyber-security.[46] The strategy involves three OAS groups which address cyber-security from a different perspective: the Inter-American Committee against Terrorism (CICTE) which supports member states in their efforts to create CSIRTs, promotes the creation of a Secure Hemispheric Network of National CSIRTs and fosters a culture of cybersecurity, the Meetings of Justice or Other Ministers or Attorneys of the Americas (REMJA) Cyber Crime Working Group which focuses on legal requirements and investigation capabilities, and the Inter-American Telecommunications Commission (CITEL) which addresses technical aspects.

- United Nations (UN)

The United Nations has been the host of a number of activities related to cybersecurity and cybercrime in the past few years.[47] In 2003, through the resolution 58/32, the General Assembly requested the Secretary-General to consider threats to information security and possible cooperative measures. To this end a Group of Governmental Experts (GGE) was established in 2004 but consensus was not reached on a final report. The same theme was discussed by a "Group of Governmental Experts", appointed in 2009 in pursuance of UN General Assembly resolution 60/45 of 8 December 2005. The Group produced a report on 16 July 2010 which recommends, among other things, "*further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructures*". In preparation of the 12th United Nations Congress on Crime Prevention and Criminal Justice[48] (Salvador, Brazil, 12-19 April 2010) the Secretariat of the UN Office on Drugs and Crime (UNODC) prepared a working paper in which it recommended that "*the development of a global convention against cybercrime should be given careful and favourable consideration*". While some countries were supporting such development, others strongly opposed highlighting the existence of the Budapest Convention and the need to focus on capacity-building rather than on law-making.

Lastly a proposal for a UN General Assembly resolution on an International code of conduct for information security was put forward by China, the Russian Federation, Tajikistan and Uzbekistan in September 2011. "*The text, similar to the one tabled in past years, called on Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information. New to the draft this year, […] was a provision seeking continuation of study by a group of governmental experts to be established in 2012 of existing and potential threats in the sphere of international security and possible cooperation measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures in information science*."[49] The UN General Assembly has also adopted several resolutions related to cyber-security such as Resolution 57/239 on the "Creation of a global culture of cybersecurity" which builds on the OECD 2002 Security Guidelines[50]

The International Telecommunication Union (ITU) is the specialised agency of the United Nations which is responsible for Information and Communication Technologies. Cybersecurity is considered in the "C5" World Summit on Information Society (WSIS) Action Line of the Geneva Action Plan on building confidence and security in the use of ICT. ITU was proposed as moderator/facilitator in implementing concrete projects and initiatives along this line. ITU deals also with adopting international standards to ensure seamless global communications and interoperability for next generation networks; building confidence and security in the use of ICTs; emergency communications to develop early warning systems and to provide access to communications during and after disasters, etc.

Intergovernmental initiatives

- Conferences on Cyberspace

The London Conference on Cyberspace[51] (1-2 November 2011) was meant to build on the debate on developing norms of behaviour in cyber-space, as a follow-up to the speech given by UK Foreign Minister Hague at the Munich Security Conference in February 2011 which set out a number of "principles" that should underpin acceptable behaviour on cyberspace. Follow-up Conferences are planned to be hosted by Hungary (4-5 October 2012) and Korea (2013).

- Meridian Process

The Meridian process aims to provide Governments worldwide with a means by which they can discuss how to work together at the policy level on Critical Information Infrastructure Protection (CIIP). Participation is open to all countries and targets senior level policymakers. An annual conference and interim activities are held each year to help build trust and establish international relations within the membership to facilitate sharing of experiences and good practices on CIIP from around the world.[52]

Annex II
Cybersecurity policy in the European Union

This annex provides an overview of *i)* recent developments at the European Union (EU) level, *ii)* the main EU institutions and departments involved in cybersecurity and *iii)* the main EU cybersecurity-related policy documents.

Recent developments on a cybersecurity strategy at the EU level

The European Commission and the High Representative for Foreign and Security Policy will jointly present a European Strategy for Cyber-Security by the second semester of 2012. This work will be jointly prepared by the Directorate General for Communications Networks, Content and Technology (DG CONNECT, ex DG INFSO), the Directorate General Home Affairs and the European External Action Service. The strategy will put forward both policy and regulatory measures to ensure a safe and resilient digital environment for all EU citizens, businesses and public administrations and to effectively prevent cybercrime, in respect of fundamental rights and European values.

Overview of EU institutions and departments

At the European Union level, topics relevant to cybersecurity and cybercrime are dealt with by various institutions and departments. They include:

- The *Council of the European Union* ("EU Council")[53] meets to adopt EU laws and coordinate EU policies. It is composed of national ministers from each EU country. The various aspects of cybersecurity are discussed in different Council configurations, such as Transport, Telecommunications and Energy (TTE) Council, Justice and Home Affairs (JHA) Council, Council Working Party on Civil Protection (PROCIV), COTER,[54] EU Military Committee (EUMC), and the Political and Security Committee (PSC) / Council Standing Committee on Operational Co-operation on Internal Security (COSI),

Council Working Party on Transatlantic Relations (COTRA), etc. The Secretariat General of the Council (SGC) of the European Union is involved in coordinating EU policy on civil protection. Its Directorate General Security, Safety and Communication and Information Systems is in charge of the security of SGC communications and information systems.

- The *European Parliament*[55] debates and passes EU laws with the EU Council, scrutinises other EU institutions to make sure they are working democratically, debates and adopts the EU's budget, with the EU Council. Its members are directly elected by EU's citizens and represent them. Various committees of the European Parliament[56] have an interest in certain aspects of cybersecurity including committees on Industry, Research and Energy (ITRE), Civil Liberties, Justice and Home Affairs (LIBE), Internal Market and Consumer Protection (IMCO), International Trade, Foreign Affairs (AFET), and Security and Defence (SEDE).

- The *European Commission*[57] and upholds the interests of the EU as a whole. It drafts proposals for new EU laws. It manages the day-to-day business of implementing EU policies and spending EU funds.

The main Directorates General involved in activities related to cybersecurity include:

- *Directorate General for Communications Networks, Content and Technology* (DG CONNECT, former DG INFSO) is in charge of policy activities on Network and Information Security (NIS) and on Critical Information Infrastructure Protection (CIIP), electronic signature directive, eGovernment, the Safer Internet programme, the ICT trust and security thematic of the 7th Framework for Research and Technological Development (FP7) and the EU Regulatory Framework for Electronic Communications.

- *Directorate General Home Affairs* (HOME) leads policies on fighting cybercrime and on the European Programme for Critical Infrastructures Protection (EPCIP).

- *Directorate General Justice* (JUST) is in charge of the EU Personal Data Protection framework;

- *Directorate General Enterprise and Industry* (ENTR) is in charge of EU industrial policy, satellite navigation, standardisation and the security thematic of FP7.

- *Directorate General Internal Market* (MARKT) is responsible for the Electronic Commerce Directive and for European legal frameworks in the areas of regulated professions, services, company law and corporate governance, public procurement, intellectual, industrial property and financial services.

- The *European Commission Joint Research Center* (JRC) provides independent, evidence-based scientific and technical support throughout the whole policy cycle. Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Several other Commission bodies are involved in cybersecurity activities focusing on the functioning of the Commission itself:

- *Secretariat General* (SG) leads activities on crisis management.

- *Directorate General for Informatics* (DIGIT) is in charge of the IT Strategy of the European Commission and of promoting and facilitating the deployment of pan-European *e*-Government services for citizens and enterprises.

- *Directorate General Human Resources and Security* (HR) lays down the European Commission policy on security and hosting a Cyber Attack Response Team (CART).

- The *European External Action Service*[58] (EEAS) assists the High Representative of the Union for Foreign Affairs and Security Policy who chairs the Foreign Affairs Council and conducts the common foreign and security policy, also ensuring the consistency and coordination of the EU's external action. EEAS is involved in international aspects related to cyber security and cybercrime.

- The *European Network and Information Security Agency*[59] (ENISA) was established in 2004 to ensure a high level of network and information security in the EU by giving expert advice on network and information security to national authorities and EU institutions, acting as a forum for sharing best practice, facilitating contacts between EU institutions, national authorities and businesses. Together with EU institutions and national authorities, ENISA seeks to develop a culture of network and information security across the EU. To assist the EU Member States in the task of developing and maintaining a successful national cybersecurity strategy, ENISA is developing a Good Practice Guide.[60]

- *EUROPOL*[61] became fully operational in 1999 as the European Union law enforcement agency that handles the exchange and analysis of criminal intelligence. Its mission is to improve the effectiveness and cooperation between EU law enforcement authorities in preventing and combating serious international crime and terrorism, with the aim of achieving a safer Europe for all EU citizens. Fighting cybercrime is one of the areas of experience of Europol. In March 2012, the European Commission proposed to establish the (future) European Cybercrime Centre (EC3)[62] within Europol.
- The *European Defence Agency* (EDA)[63] was established in 2004 to improve the EU's defence capabilities especially in the field of crisis management; promote EU armaments co-operation; strengthen the EU defence industrial and technological base and create a competitive European defence equipment market; promote research, with a view to strengthening Europe's industrial and technological potential in the defence field.
- The *EU Institute for Security Studies* (EUISS)[64] is an autonomous agency that is an integral part of the support structures for the EU's Common Foreign and Security Policy (CFSP). It provides analyses, forecasts and recommendations on security issues of relevance for the EU. It provides a forum for debate between European experts and decision-makers at all levels.
- The *European Data Protection Supervisor* (EDPS) [65] was created in 2001 to ensure that all EU institutions and bodies respect people's right to privacy when processing their personal data.
- *Pre-configuration team* of the *Computer Emergency Response Team* for the EU Institutions and bodies.[66] This EU inter-institutional team was established in June 2011 to help European Institutions and bodies to protect themselves against non-intentional incidents and malicious attacks on their IT assets. Its scope of activities covers Announcements, Alerts and Incident Response Co-ordination.

Main EU policy documents related to cybersecurity

General documents

- EC (2001), Communication on "Network and Information Security: Proposal for A European Policy Approach", COM(2001)298. Available at *http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf*

- EC (2006), Communication on a "Strategy for a Secure Information Society - Dialogue, partnership and empowerment", COM(2006)251. Available at *http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf*.
- EC (2009), Directive 2009/140/EC of the European Parliament and of the Council amending Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive). Available at *http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf*. This Directive sets new provisions on security and integrity of networks and services. See Art. 13 a and b of the Framework Directive.
- EC (2010), "A Digital Agenda for Europe", COM(2010) 245 final/2. Available at *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF*. See the Trust and Security chapter which launched several actions addressing security and resilience.
- EC (2010), "Delivering an area of freedom, security and justice for Europe's citizens. Action Plan Implementing the Stockholm Programme", COM(2010) 171 final. Available at *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:EN:PDF*.
- EC (2010), "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe", COM(2010) 673 final. Available at *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF*. The Stockholm Programme/Action Plan and the EU Internal Security Strategy in action underline the Commission's commitment to building a digital environment where every European can fully express his or her economic and social potential.
- EC (2010), Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, COM(2010) 517. Available at *http://ec.europa.eu/home-affairs/policies/crime/1_EN_ACT_part1_v101.pdf*.

ENISA

- EC (2004), "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 (ENISA)". Available at *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=-CELEX:32004R0460:EN:HTML*.

- EC (2010), "Proposal for a regulation concerning the European Network and Information Security Agency (ENISA)". Available at *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF*.

CIIP

- EC (2006), "Communication on a European Programme for Critical Infrastructure Protection (EPCIP)", COM(2006)786. Available at *http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf*

- EC (2009), "Communication on Critical Information Infrastructure protection (CIIP). Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009) 149 final. Available at *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF*.

- EC (2011), "Communication on Critical Information Infrastructure Protection. Achievements and next steps: towards global cyber-security", COM(2011) 163 final. Available at *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF*. This second communication on CIIP takes stock of the results achieved since the adoption of the CIIP action plan in 2009 and describes the next priorities planned under each action at both European and international level.

Protection of children

- Official Journal of the EU (2011), Directive 2011/92/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography. Available at *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF*. This Directive replaces Council Framework Decision 2004/68/JHA.

- European Parliament and Council (2008), Decision No 1351/2008/EC of 16 December 2008 establishing a multi-annual Community programme on protecting children using the Internet and other communication technologies. Available at *http://ec.europa.eu/information_society/activities/sip/docs/prog_decision_2009/decision_en.pdf*.

Annex III
Key policy documents per country[67]

Australia	• Cyber Security Strategy. Australian Government, 2009. • Connecting with Confidence, Optimising Australia's Digital Future. Australian Government, 2011.[68]
Canada	• Canada's Cybersecurity Strategy: For a Stronger and More Prosperous Canada. Government of Canada, 2010. • National Strategy for Critical Infrastructure and Action Plan for Critical Infrastructure. Government of Canada, 2009.
Finland[69]	• National Security Strategy for Society. Finnish Ministry of Defense, 2010. • Government Resolution on Enhancing Information Security in Central Government, VAHTI 7/2009. Finnish Ministry of Finance, 2009.
France	• Defence and Security of Information Systems. Strategy of France. Prime Minister's Secretary General for Defence and National Security, 2011. • White Book on Defence. French Government, 2008. • Main measures adopted by the government. French *Conseil des Ministres*, 2011.
Germany	• Cyber Security Strategy for Germany. German Federal Ministry of the Interior, 2011.
Japan	• Information Security Strategy for Protecting the Nation. Japanese Information Security Policy Council, 2010.[70] • Annual Plan Information Security. Japanese Information Security Policy Council, 2010. • Second Action Plan on Information Security Measures for Critical Infrastructures. Information Security Policy Council, 2009. • Policy for Enhancement of Information Security Measures for the Central Government Computer System. Japanese Information Security Policy Council, 2005. • Standards for Information Security Measures for the Central Government Computer System. Japanese Information Security Policy Council, 2010.
Netherlands	• The National Cyber Security Strategy. Dutch Ministry of Security and Justice, 2011.

Spain[71]	• Spanish Security Strategy: Everyone's responsibility. Gobierno de España, 2011. • Royal Decree 3/2010 of 8 January 2010, regulating the National Security Framework within the scope of e-government; Law 8/2011 of 28 April 2011, establishing measures for the protection of critical infrastructures; Royal Decree 704/2011 of 20 May 2011, approving secondary legislation on the protection of critical infrastructure; Law 59/2003 of 19 December 2003, on electronic signature; Royal Decree 1553/2005 of 23 December 2005 regulating the issuance of the national identity card and its electronic signature certificate.
United Kingdom	• The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world. UK Cabinet Office, 2011. • Cyber Security Strategy of the United Kingdom. Safety, Security and Resilience in Cyber Space. UK Cabinet Office, 2009. • Strategic Defence and Security Review (SDSR). UK Prime Minister, 2010. • A Strong Britain in an Age of Uncertainty: The National Security Strategy. UK Prime Minister, 2010. • Cyber Crime Strategy. Home Office, 2010.
United States	• Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure. White House, 2009. • International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. White House, 2011. • Cybersecurity Legislative Proposal. White House, 2011. • Comprehensive National Cybersecurity Initiative. White House, 2010. • Department of Defense Strategy for Operating in Cyberspace. Department of Defense, 2011. • Cybersecurity, Innovation and the Internet Economy. Department of Commerce, 2011. • National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security and Privacy. White House, 2011. • Trustworthy Cyberspace: Strategic Plan for the Federal cybersecurity Research and Development Program. Executive Office of the President, National Science and Technology Council, 2011.

Annex IV
Key objectives and concepts in cybersecurity strategies

Australia	• Maintain a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy. • All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finance online • Australian businesses operate secure and resilient ICTs to protect the integrity of their own operations and the identity and privacy of their customers • The Australian Government ensures its ICTs are secure and resilient
Canada	• Securing Government systems • Partnering to secure vital cyber systems outside the federal Government • Helping Canadians to be secure on line.
Finland[72]	• By 2016, Finland is global forerunner in cyber threat preparedness and in securing vital functions of the society under all circumstances. • Finland is an active player in international co-operation for cybersecurity strategy. • Security and reliable cyberspace is more an enabler than a threat. • Focus on vital functions for the Finnish society: government functions, international activities, defense, internal security, functioning of the economy and infrastructure, population's income security and capacity to functions, psychological resilience to crisis.
France	• Becoming a world "cyberdefence" power. • Guarantee freedom of decision of the country by protecting sovereignty information (*i.e.* "diplomatic, military, scientific, technical and economic information which enables freedom of action and conditions prosperity of nations"). • Reinforce cybersecurity of national critical infrastructures • Ensure security in cyberspace.

Germany	• Maintain and promote economic and social prosperity • Ensure cybersecurity at a level commensurate with the importance and protection required by interlinked information infrastructures, without hampering opportunities and the utilisation of cyberspace
Japan	• Reinforce policies taking account of possible outbreaks of cyber attacks (reinforce the general mode of readiness) and establish counteractive organisation.
Netherlands	Strength through co-operation: • Interlinking and strengthening initiatives • Public private partnerships • Individual responsibility • Division of responsibilities between ministries • Active international co-operation • Measures must be proportionate • Self-regulation if possible, legislation if necessary.
Spain	• Strengthened regulation. • Public-Private partnership. • Culture of cybersecurity. • Improved national and international co-ordination. • Development of a risk map and catalogue of experts, resources and best practices. • Consolidation of the National Critical Infrastructure Protection Plan. • Implementation of the National Security Framework. • Provision of citizens with strong e-authentication and e-signature capabilities. • Standardisation and certification. • Recognition of a safe cyberspace as a competitive edge for the country.
United Kingdom	Derive huge economic and social value from a vibrant, resilient and secure cyberspace where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society. • Tackle cyber crime and be one of the most secure places in the world to do business in cyberspace • Be more resilient to cyber attacks and better able to protect our interests in cyberspace • Have helped to share an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies • Have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber objectives.

United States	• Establish leadership at the highest level (White House). • Establish a national dialogue on cybersecurity, engage in a global race depending on mathematics and skills (like after the launch of Sputnik in 1957). • Enhance partnerships with private sector, clarify roles and responsibilities. • Address the cross-border challenge by shaping the international environment, and bringing like-minded nations together. • Develop a comprehensive framework to ensure a coordinated response by the Federal, State, local and tribal governments, the private sector and international allies to significant incidents. • Define performance and security objectives for the next generation infrastructure, with the private sector.

Annex V
Questionnaire circulated to volunteer countries

1. What is your cybersecurity strategy?

This question aims to gather information on the strategy itself and the rationale behind it. Please provide details, as appropriate, including for example on:

- The objectives of the strategy, its scope, main components, the main drivers and contextual changes that led to its development, and the meaning or understanding of "cybersecurity" in this particular context.
- The international dimension of your strategy, including in relation to international organisations.
- The elements of your strategy that are entirely new or significantly different from the past.
- What your government considers as the main priorities.

2. What are you doing to implement the strategy?

This question aims to help us understand what policies have been (or are expected to be) developed or significantly modified as a consequence of the adoption of your strategy.

Please:

- Explain how your policies reflect your strategy, with a focus on those policies which are new or which have been significantly modified.
- Provide information on the international aspects of the implementation of your strategy.

3. How do you achieve policy coherence and consistency across the full range of government responsibilities?

This question aims to gather information on how cybersecurity strategies and policies both protect the economy and the society, and actively foster economic and social development.

Please provide details, as appropriate, on:

- The structures and processes that ensure coherence and consistency of cybersecurity strategies and policies with strategies and policies in other areas, *i.e.* economy (*e.g.* innovation, growth, competition), protecting national interests (or "national security"), education, research and development, e-government, and fundamental values (*e.g.* good governance, privacy, free flow of information, etc.).
- The main challenges in achieving such coherence and consistency.

4. What processes are (were or plan to be) used to develop, implement and review the strategy and policies?

Please describe the processes for the *i)* development, *ii)* implementation, *iii)* review of your strategy and policies, *iv)* measurement of their effectiveness and *v)* involvement of stakeholders in the development, implementation and review of your strategy and policies.

Please also highlight:

- Who are the major stakeholders and what is their role.
- Where appropriate, the role of international co-operation (*e.g.* regional or international exercises) and international organisations, as well as your participation in international co-operation.
- The main challenges and enablers that your government has faced or is facing in the process of development, implementation and review of its strategy and policy, as well as in the process for international co-operation.
- If your strategy and/or policies have already been evaluated, what lessons have been learned?

Annex VI
Questionnaire circulated to non-governmental stakeholders

The questionnaire below aimed to collect input from business and industry, civil society and the Internet technical community to understand their perspective on national cybersecurity strategies analysed in the report. This consultation was channelled through the official representation of these stakeholder communities to the OECD: the Business and Industry Advisory Committee to the OECD (BIAC), Civil Society Internet Society Advisory Council (CSISAC) and the Internet Technical Advisory Committee (ITAC).

From your perspective:

1. What are the main cybersecurity challenges, priorities, and goals for the economy and the society?
2. What is the role and responsibility of governments with respect to public policy for cybersecurity? What do you see as the most important evolutions in government strategies?
3. How should governments implement cybersecurity policy at national and at international levels and how does this compare with current new strategies?
4. What is the role and responsibility of [business and industry] [civil society] [the Internet technical community] with respect to cybersecurity public policy? How is this reflected in the new strategies?
5. What is -or what will be- the impact of recent cybersecurity strategies on [business and industry] [civil society] [the Internet technical community]?
6. How should national cybersecurity strategies and policies be evaluated? What metrics should be applied to measure their efficiency?

Notes

1. The material for this analysis was collected between March 2011 and March 2012.
2. Business and Industry Advisory Committee (BIAC), the Civil Society Internet Society Advisory Council (CSISAC) and the Internet Technical Advisory Committee (ITAC) to the OECD.
3. Specific issues related to the protection of critical information infrastructures are not addressed in this report although they appear in some strategies. See *the OECD Recommendation on the Protection of Critical Information Infrastructures (2008).*
4. Annex III provides an overview of intergovernmental organisations addressing cybersecurity. Annex IV describes initiatives in the European Union.
5. See OECD, 2005.
6. References to the views of "business", "civil society" and the "Internet technical community" reflect input from, respectively, BIAC, CSISAC and ITAC. The full text of their responses to this questionnaire is available separately (OECD, 2012b).
7. The analysis below includes Finland and Spain taking into account that they have not yet adopted a cybersecurity strategy. Most of the information related to these two countries' approach is related to their national security strategy and/or other key policy documents provided by delegations. These elements provide an indication of the direction of their future cybersecurity strategy.
8. See Annex IV.
9. See OECD, 2009.
10. In this paper, the term attack refers to any type of intentional exploitation of a vulnerability by a source of threat, including for breach of confidentiality.
11. Government of Canada, 2010, p. 6.
12. This dependence characterises the concept of "critical information infrastructure" as defined in the OECD Recommendation on Critical Information Infrastructure Protection. See OECD, 2008.

13. For Japan, the increasing dependency on ICT in socioeconomic activities implies that "information security can be seen as a part of the social infrastructure".

14. The Spanish Security Strategy, which addresses all national security risks, considers cyberspace as a specific domain comparable to land, sea, air, space and information, and which includes the Internet as well as cellular phones, terrestrial television and satellite communications.

15. The French approach to "cyberdefense" includes all aspects of cyber-security, regardless of their military or civilian nature. ANSSI, which sits under a Prime Minister's co-ordination body for matters of national security and defense, is the national authority for cybersecurity.

16. See ENISA, 2011c.

17. GBP 650 million.

18. "While securing peace of mind for the nation's citizens by implementing measures to protect personal information and improve security, Japan will make every effort to encourage utilization of information and communications technology, such as through improved training to provide people with a command of this technology. This will make daily life more convenient for the public, triple productivity in fields concerned with information and communications technology, enhance international competitiveness by lowering production costs, and foster the development of new industries" (Japanese Cabinet Office, 2010).

19. The Dutch strategy adds that legislation should not distort competition, not increase the administrative burden disproportionately, leads to a favourable cost-benefit ratio and ensures a level playing field.

20. For example in relation to export controls or simply because of the use of IT by the military and the intelligence community, as demonstrated by the development of Internet technologies by the US Defense Advanced Research Projects Agency (DARPA).

21. For example, its Strategic Initiative 3 states that "DoD will partner with other US government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy" (US DoD, 2011, p. 8).

22. "Civilian cybersecurity focuses on all IT systems for civilian use in German cyberspace. Military cybersecurity focuses on all IT systems for military use in German cyberspace." (German Federal Ministry of the Interior, 2011).

23. See ENISA, 2011a, p.12.

24. See *www.dpmc.gov.au/national_security/index.cfm* and *www.dpmc.gov.au/annual_reports/2010-11/html/chapter-04/02-nscio.cfm*.

25. See www.ag.gov.au/Cybersecurity/Pages/default.aspx.

26. See www.ssi.gouv.fr.

27. *Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».*

28. See www.cabinetoffice.gov.uk/content/office-cyber-security-and-information-assurance-ocsia.

29. See also Council of Europe, 2011 for a discussion on the concepts of cybercrime and cybersecurity strategies.

30. The Cyber Security Challenge is a non-profit public-private initiative that "runs national online competitions and raises awareness of cyber learning opportunities and careers. It is designed to excite, inspire and help talented people, of any age, to follow a career in cyber security". See :https://cybersecuritychallenge.org.uk.

31. ibid, 4.47.

32. Another initiative which is not part of a government national cybersecurity strategic plan but may act as a market incentive is the issuance by the US Securities and Exchange Commission (SEC) of Guidance regarding disclosure obligations relating to cybersecurity risks and cyber incidents (US Securities and Exchange Commission, 2011).

33. However, it was not mentioned by Spain despite its large scale electronic national identity card rollout plan. This is consistent with the findings of the OECD comparative analysis of national strategies for digital identity management. See OECD, 2011.

34. See OECD, 2011. About De-mail, see www.bsi.bund.de/DE/Themen/EGovernment/DeMail/DeMail_node.html (in German) and http://en.wikipedia.org/wiki/De-Mail.

35. Examples provided by the Internet technical community include, from IETF, DNSSEC, TLS, IPSec, RPKI, SAML; from W3C, Content Security Policy, XML Signature, XML encryption; from OASIS, Digital Signature Services (DSS), Security Assertion Markup Language (SAML); from ISO, security management standards such as IS27001 and IS27002 as well as the Entity Authentication Assurance Framework, DIS29115.

36. See *www.safecode.org* and *http://www3.opengroup.org/getinvolved/forums/trusted*

37. Some of the largest defense and security firms (*e.g*. Boeing, EADS, Finmeccanica, Lockheed Martin, Northrop Grumman, Thales, …) have a portfolio of cybersecurity products and services which extends beyond government military markets to civilian customers.

38. A list of organisations addressing cybersecurity standardisation can be found in the *ICT Security Standards Roadmap* developed by ENISA, ITU and the Network and Information Security Steering Group (NISSG) of the ICT Standards Board.
See *www.itu.int/ITU-T/studygroups/com17/ict/part01.html*.

39. See www.apec.org

40. See:
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=04/04/2012&CL=ENG

41. See,
www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp.

42. See, *www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html*

43. See *www.intgovforum.org/cms/aboutigf*.

44. See *www.ccdcoe.org*.

45 . See *www.osce.org/atu/44197*.

46 . See
www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

47 . See an exhaustive review of the activities of the UN regarding cyber-security at: *www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf*

48. *www.unodc.org/unodc/en/crime-congress/12th-crime-congress.html*.

49. See *www.un.org/News/Press/docs/2011/gadis3442.doc.htm*.

50. See *www.oecd.org/dataoecd/53/60/37019786.pdf*.

51. See *www.fco.gov.uk/en/global-issues/london-conference-cyberspace/*.

52 . See *www.meridianprocess.org.*

53. See *www.consilium.europa.eu*

54. COTER brings together Member States' experts from foreign affairs ministries to focus on the external aspects of terrorism.

55. See *www.europarl.europa.eu/portal/en*

56. See *www.europarl.europa.eu/committees/en/parliamentary-committees.html*

57. See *http://ec.europa.eu/index_en.htm*

58. See *http://eeas.europa.eu*.

59. See *www.enisa.europa.eu*.

60. See *www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss*

61. See *www.europol.europa.eu*.

62. See *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF*.

63. See *www.eda.europa.eu.*

64. See *www.iss.europa.eu*.

65. See *www.edps.europa.eu*

66. See *http://cert.europa.eu/cert/plainedition/en/cert_about.html*

67 . See hyperlinks in the References section.

68 . See also Conroy, 2011.

69 . Cybersecurity strategy is being developed. These documents form the current basis on which the strategy will be built.

70 . The strategy has been updated in 2011 by the "Information Security 2011", available at www.nisc.go.jp/eng/pdf/is2011_eng.pdf. Another update was released in 2012 and will be published in English in the second part of the year. The "Management Standards for Information Security Measures for the Central Government Computer Systems" (April 2011), available at www.nisc.go.jp/eng/pdf/K304-101e.pdf, updates the "Standards for Information Security Measures for the Central Government Computer system" of 2010 and the "Policy for Enhancement of Information Security Measures for the Central Government" of 2005.

71 . Cybersecurity strategy is being developed. These documents form the current basis on which the strategy will be built.

72 . The Finnish cybersecurity strategy is under development at the time of writing.

References

ANSSI (2011), "*Défense et sécurité des systèmes d'information. Stratégie de la France"*. Available at *www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf*.

Australian Government (2009), "Cyber Security Strategy". Available at *www.ag.gov.au/www/agd/rwpattach.nsf/VAP/%284CA02151F94FFB778ADAEC2E6EA8653D%29~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf*.

Australian Government (2011), "Connecting with Confidence. Optimising Australia's Digital Future". Available at *http://cyberwhitepaper.dpmc.gov.au/sites/default/files/documents/connecting_with_confidence_public_discussion_paper.pdf.*

Conroy S. (2011), Joint Media Release. Cyber White Paper. Available at *www.minister.dbcde.gov.au/media/media_releases/2011/198*.

Council of Europe (2011), "Cybercrime strategies". Discussion paper prepared by the Global Project on Cybercrime. Available at *www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf.*

Dutch Ministry of Security and Justice (2011), The National Cyber Security Strategy (NCSS). Strength through cooperation. Available at http://english.nctb.nl/Images/cyber-security-strategy-uk_tcm92-379999.pdf.

ENISA (2011a), "Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report", p. 12. Available at *www.enisa.europa.eu/act/res/other-areas/metrics/reports/metrics-tech-report/at_download/fullReport.*

ENISA (2011b), "Country Reports". *Available at www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/*

ENISA (2011c), "Cyber security: future challenges and opportunities". Available at *www.enisa.europa.eu/publications/position-papers/cyber-security-future-challenges-and-opportunities*.

ENISA (2012), "National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace". Available at *www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper.*

European Union (2012), "Neelie Kroes. A European Strategy for Internet Security. High Level Public-Private Security Roundtable. Brussels, 21st March 2012". Available at *http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/204*.

Finnish Ministy of Defense (2010), "Security Strategy for Society. Government Resolution 16.12.2010". Available at *www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/26-security-strategy-for-society*.

Finnish Ministry of Finance (2009), "Government Resolution on Enhancing Information Security in Central Government". VAHTI 7/2009. Available at *www.vm.fi/vm/en/04_publications_and_documents/01_publications/05_government_information_management/20091126Govern/Vnpp_enkku.pdf*.

French Government (2008), *Livre Blanc de la Défense Nationale*. Odile Jacob, Paris. Available at *www.livreblancdefenseetsecurite.gouv.fr/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/index.html*.

French *Conseil des Ministres* (2011), *Conseil des Ministres du 25 mai 2011*. "*Principales mesures adoptées par le gouvernment"*. Available at *www.ssi.gouv.fr/IMG/pdf/2011-05-25_principales_mesures.pdf*.

German Federal Ministry of the Interior (2011), "Cyber Security Strategy for Germany". Available at *www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile.*

Gobierno de España (2011), "Spanish Security Strategy. Everyone's responsibility". Available at *www.lamoncloa.gob.es/NR/rdonlyres/EF784340-AB29-4DFC-8A4B-206339A29BED/0/SpanishSecurityStrategy.pdf*.

Government of Canada (2010), Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada. Available at *www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-eng.aspx*.

Government of Canada (2009), Action Plan for Critical Infrastructure. Available at *www.publicsafety.gc.ca/prg/ns/ci/ct-pln-eng.aspx.*

Government of Canada (2009), National Strategy for Critical Infrastructure. Available at *www.publicsafety.gc.ca/prg/ns/ci/ntnl-eng.aspx*.

Japanese Information Security Policy Council (2010), "Information Security Strategy for Protecting the Nation". Available at *www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf*.

Japanese Information Security Policy Council (2010), Annual Plan Information Security 2010. Available at *www.nisc.go.jp/eng/pdf/is2010_eng.pdf*. [The Annual Plan for 2011 is available at *www.nisc.go.jp/eng/pdf/is2011_eng.pdf*. The Annual Plan for 2012 will be available in English in the second part of 2012].

Japanese Cabinet Office (2010), "New Growth Strategy". Available at *www.meti.go.jp/english/policy/economy/growth/report20100618.pdf*.

Luiijf, H., Besseling, K., Spoelstra, M., Graaf, P. de (2011), *Ten National Cyber Security Strategies: a comparison*. CRITIS 2011 – 6th International Conference on Critical information infrastructures Security, September 2011.

Lynn W. J. (2010), "Defending a New Domain. The Pentagon Cyberstrategy", in *Foreign Affairs*, September-October 2010.

OECD (2002), *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security,* Paris. Available at *www.oecd.org/document/42/0,3746,en_2649_34255_15582250_1_1_1_1,00.html*.

OECD (2005), *The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries*, Paris. Available at *www.oecd.org/dataoecd/16/27/35884541.pdf.*

OECD (2008), *Recommendation of the Council on the Protection of Critical Information Infrastructures*, Paris. Available at *www.oecd.org/dataoecd/1/13/40825404.pdf.*

OECD (2009), *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy*, OECD Publishing. doi: 10.1787/9789264056510-en.

OECD (2011), *National Strategies and Policies for Digital Identity Management in OECD Countries*, OECD Digital Economy Papers, No. 177, OECD Publishing. http://dx.doi.org/10.1787/5kgdzvn5rfs2-en.

OECD (2012a), "Proactive Policy Measures by Internet Service Providers against Botnets", OECD Digital Economy Papers, No. 199, OECD Publishing. http://dx.doi.org/10.1787/5k98tq42t18w-en.

OECD (2012b), "Non-Governmental Perspectives on a New Generation of National Cybersecurity Strategies". Contributions from BIAC, CSISAC and ITAC. [DSTI/ICCP/REG(2012)7] (Unclassified)].

UK Cabinet Office (2009), "Cyber Security Strategy of the United Kingdom. Safety, Security and Resilience in Cyber Space". Available at *www.cabinetoffice.gov.uk/media/216620/css0906.pdf*.

UK Cabinet Office (2011a), "The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world". Available at *www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy*.

UK Cabinet Office (2011b), "Government Cloud Strategy. A sub strategy of the Government ICT Strategy". Available at *www.cabinetoffice.gov.uk/sites/default/files/resources/government-cloud-strategy_0.pdf*.

UK Foreign and Commonwealth Office (2011), "Security and freedom in the cyber age - seeking the rules of the road". Available at *www.fco.gov.uk/en/news/latest-news/?view=Speech&id=544853682*.

UK Home Office (2010), "Cyber Crime Strategy". Available at *www.official-documents.gov.uk/document/cm78/7842/7842.pdf*.

UK Prime Minister (2010a), "Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review". Available at *http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/intelligence-security-resilience/national-security/strategic-defence-security-review.aspx*.

UK Prime Minister (2010b), "A Strong Britain in an Age of Uncertainty: The National Security Strategy". Available at *www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy*.

US Department of Commerce (2011), "Cybersecurity, Innovation and the Internet Economy". Available at *www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf*.

US Department of Defense (2011), "Department of Defense Strategy for Operating in Cyberspace". Available at *www.defense.gov/news/d20110714cyber.pdf*.

US Executive Office of the President, National Science and Technology Council (2011), "Trustworthy Cyberspace: Strategic Plan for the Federal cybersecurity Research and Development Program". Available at

www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf.

US House of Representatives. Permanent Select Committee on Intelligence (2011), "Rogers & Ruppersberger Introduce Cybersecurity Bill to Protect American Businesses from "Economic Predators". Available at *http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/113011CyberSecurityLegislation.pdf*.

US Securities and Exchange Commission (2011), CF Disclosure Guidance: Topic No. 2. Cybersecurity. Available at *www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.*

US White House (2009), Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure. Available at *www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf*.

US White House (2010), The "Comprehensive National Cybersecurity Initiative". Available at *www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative*.

US White House (2011a), "International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World". Available at *www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf*.

US White House (2011b), "National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security and Privacy". Available at *www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf*.

US White House (2011c), Fact Sheet: "Cybersecurity Legislative Proposal". Available at *www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal*.

NON-GOVERNMENTAL PERSPECTIVES ON A NEW GENERATION OF NATIONAL CYBERSECURITY STRATEGIES:

CONTRIBUTIONS FROM BIAC, CSISAC AND ITAC

Note by the Secretariat

This document brings together views from business, civil society and the Internet technical on the emergence of a new generation of national cyber-security strategies. These stakeholder views were solicited in January 2012 by the OECD Secretariat through a questionnaire to the Business and Industry Advisory Committee (BIAC), the Civil Society Internet Society Advisory Council (CSISAC) and the Internet Technical Advisory Committee (ITAC) to the OECD. This input was used in developing the report on "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy" which was declassified in November 2012 by the OECD Committee on Information, Computer and Communications Policy (ICCP). These views will also inform the review of the 2002 *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* undertaken by the Working Party on Information Security and Privacy (WPISP) in 2012-2013.

About the OECD ICCP non-governmental stakeholder representation

Business and Industry Advisory Committee (BIAC) - www.biac.org

Founded in 1962, the Business and Industry Advisory Committee to the OECD (BIAC) is officially recognised by the OECD as the representative body of the OECD business community. As an independent international business association, BIAC brings a cross-sectoral and multidisciplinary view to OECD work most relevant to business. It systematically engages over 2100 business representatives, from 49 national business organisations in OECD member countries and major non-member economies, as well as 29 sectoral supra-national associations.

Civil Society Internet Society Advisory Council (CSISAC) – csisac.org

The Civil Society Information Society Advisory Council (CSISAC) contributes constructively to the policy work of the OECD ICCP Committee and promotes the exchange of information between the OECD and the civil society participants most active in the field of information technology. Information from the OECD will provide civil society participants with a stronger empirical basis to make policy assessments; inputs into research and policy development from civil society will provide the OECD with the

essential perspective of stakeholders "at the receiving end" of policy. Strengthening the relationship between civil society and the OECD will lead to better-informed and more widely accepted policy frameworks.

Internet Technical Advisory Committee (ITAC) – www.internetac.org

The Internet Technical Advisory Committee to the OECD (ITAC) brings together the counsel and technical expertise of technically focused organisations, in a decentralised networked approach to policy formulation for the Internet economy. The main purpose of the ITAC is to contribute constructively to the OECD's development of Internet-related policies. ITAC primarily contributes to the work of the OECD Committee for Information, Computer and Communications Policy (ICCP) and its specific working parties such as the Working Party on Communications and Infrastructure Services Policy (CISP), the Working Party on Information Economy (WPIE) and the Working Party on Information Security and Privacy (WPISP). The ITAC is open to any Internet technical and research organisation that meets the membership criteria listed in the Committee's Charter.

Non-Governmental Perspectives on a New Generation of National Cybersecurity Strategies: Contributions from BIAC, CSISAC and ITAC

From your perspective:

1) What are the main cybersecurity challenges, priorities, and goals for the economy and the society?

Response from BIAC

We all recognise the increasing complexity of systems and the increasing interactivity among and across systems. This increasing complexity and interaction is essential to support and incent many of the economic and societal benefits that exist in our digital economy and information society. This complexity and interaction is also more difficult to secure. There are new and multiplying threat vectors from more professional and criminally oriented actors than ever before. We have also seen the global nature of exploits increasing with computer and mobile exploits morphing across the globe like natural viruses do in epidemics, except at Internet speed. Our available reaction time to contain and address these problems has become significantly reduced and constrained.

Going forward we clearly understand the need to continue to increase efforts to reduce cybercrime, increase security in products and services, and advance risk management practices address these issues to assure continued trust in the infrastructure, the creation of new and innovative products and services and continued growth in and adoption of new technologies, services and business models predicated on the open Internet.

Major challenges include:

- A globally distributed, sometimes coordinated, and increasingly professional group of bad actors that use increasingly sophisticated means to deny service or steal, alter or destroy information.
- We note that the geographic distribution of the perpetrators of cyber-attacks makes it very difficult to pinpoint one geographical

location as the origin of these attacks; the ubiquitous connectivity of Cyberspace poses a challenge regarding the effectiveness of counter-measures which tend to be short lived since it is sufficient to simply regroup the malicious resources and start again.

- Diminished lead and reaction time to threats including potential zero day exploits.
- Complex systems and interactions among systems that may increase the challenge and complexity of security.
- The increasing national mandates for using local standards or technologies will hurt security and limit innovation.
- The world economy and the security of sovereign states benefits from international risk-based standards.
- The increased challenges of effectively and globally sharing information related to threats or exploits, while assuring that such sharing does not enhance the potential success of threats or exploits.
- Assuring that data is properly secured in systems in a holistic and defense in depth manner across all relevant control parameters.
- Fostering better security by design across government and industry and addressing the explosion of new individual application developers who may have little formal training in writing code or securing software.
- Training at all levels of the organisation on security appropriate to their role; focusing on both technical and human factors.
- Training of individual users appropriate to their role: updated anti-virus and malware definitions, common sense surfing tips, minimal steps to protect identity and sensitive information; alerts on phishing and social engineering.
- Information sharing related to terrorist or criminal acts between government and industry that both meets national security/law enforcement requirements while respects the relevant privacy and civil liberties limitation on information sharing.
- The lack of "inter-operability" between the legal frameworks adopted by different countries increases the difficulty in defining a global solution to combat cybercrime and prevent the misuse of information; this results in a "nomadic cybercrime" since cyber-criminals cannot be bound to any territorial jurisdiction.

The above challenges can only successfully be addressed if innovation in technology and security are allowed to advance. Furthermore, these challenges should not be addressed through top down proscriptive measure that result in technology mandates or unnecessarily interfere with the development and deployment of systems. Importantly, in tackling security challenges one of the priorities is to promote the use of appropriate risk assessment frameworks to evaluate the potential negative impacts to critical information infrastructures caused by security threats and vulnerabilities. The most important actions should be focused to ensure the availability, reliability and security of networks and information systems.

Cybersecurity must have the objective to achieve a distributed and co-ordinated approach to provide the level of security and resilience that is needed in cyberspace. Efforts to improve cybersecurity should be based on globally accepted standards, best practices, and international assurance programs. This approach will improve security, because proven and effective security measures must be deployed across the entire global infrastructure. Another goal of this approach is to improve interoperability of the digital infrastructure, to incentivise more private-sector resources to be used for investment and innovation to address future security challenges.

Lastly, organisations must often work globally and across sectors. This must be done using globally coherent systems and common practices based on international standards. Efforts to create national or local implementations of security, not based on internationally accepted practices, could severely increase cost, limit functionality and constrain innovation.

Response from CSISAC

Our greatest cybersecurity challenge is the overall lack of clear priorities aimed at addressing specific tangible and demonstrable harms in a targeted manner. Reliance on general and non-contextual statements of increased cyber insecurity is leading to proposals for broad, open-ended powers that threaten citizens' fundamental rights in disproportionate ways. As noted in the 2002 OECD Security Guidelines, cybersecurity initiatives should be implemented in a manner that is consistent with the rights that are essential to free and democratic societies. Many current cybersecurity initiatives fall short of this objective. Clarifying governments' priorities and goals, and ensuring a fact-based, threat-specific approach is critical to remedying this tendency and to the development of cybersecurity strategies that are beneficial to the economy and society. Such strategies should narrowly target well-defined problems that are justified on the public record. This will avoid a monolithic approach to cybersecurity that conflates many distinct issues and contexts. Untargeted approaches lacking in specificity lead to overbroad or vague powers resulting in serious threats to fundamental rights of citizens.

An effective and proportional solution will be narrowly tailored to address well-defined risks premised on risk assessments.

One great hindrance to effective policy-making in this area is the lack of publicly available, concrete information from independent sources. Part of the problem is that implementation of cybersecurity measures will often occur on private networks with scant incentive to disclose problems, and often with many incentives not to do so. Attempts to treat all potential cybersecurity issues as "threats to national security" import a culture of secrecy that further prevents public disclosure of adequate information. While there may be legitimate reasons for withholding some of this information, there must be a serious attempt at overcoming these challenges to enable fact-based decision-making as a more central component to the cybersecurity discussion.

Many recent cybersecurity proposals envision open-ended powers to monitor and react to online activity. Such powers are inconsistent with fundamental rights and freedoms, the rule of law, and legitimate interests that are core to democratic societies, and therefore lie in conflict with Principles 4 and 5 of the OECD's own security guidelines of 2002. Legal proposals that lack any exhibited safeguards or attempts to target solutions in a contextual manner are inherently disproportionate and pose an unjustifiable threat to privacy and freedom of expression. This, in turn, threatens the transparency and openness recognised in the Security Guidelines as essential to cybersecurity strategies in democratic societies.

Beyond the threat to transparency and openness of process, proposals that lack such specificity of purpose threaten the economic and societal value of the Internet. This is already evident in the implementation of previous cybersecurity strategies. In the United States, for example, cybersecurity provisions have been misused in a myriad of ways: to hinder competition and innovation, to prevent users from accessing their own data by the mechanism of their choice, to prevent users from accessing legally purchased products such as gaming systems, to shut down criticism, to deter academic research and even, somewhat counter-productively, to deter security researchers.[1] Instead of engaging in a nuanced assessment of what activities are positive and which warrant deterrence, policies grant broad powers to "prevent unauthorised access". It is then left to private companies or prosecutors to decide in what instances these powers should be used. This, in turn, leads to serious impact on fundamental rights. The same flaws are already evident in cybersecurity legislative proposals that aim to empower private companies with ill-defined "monitoring" and "countermeasure" powers.[2]

With respect to the adoption of specific initiatives, a "risk assessment first" approach is in accordance with the current 2002 OECD Security Guidelines, especially the principles on security management, risk assessments, awareness, and reassessment. Cybersecurity strategies cannot be set or assessed in the abstract. It is impossible to conduct fact-based policy-making without first assessing the parameters of the risks involved and, only then, assessing the proportionality of any proposed powers. Acceptable levels of risk can only be determined *after* factual assessments have been completed, and with the nature and importance of the information sought to be protected firmly in mind. Risk assessments should be an ongoing process because appropriate modifications to security policies need to be made to deal with new and ever-changing threats and vulnerabilities. Once governments conduct these assessments, they must then clearly articulate the tangible cybersecurity risk they are addressing in each discrete initiative. This is why cybersecurity strategies should include, as a prerequisite to the adoption of any specific cybersecurity initiative, a risk assessment leading to a clear statement of the assets to be protected and the risk models that demonstrate this need for protection.

Yet another way in which cybersecurity policies exhibit a troubling lack of specificity is in the very definition of them. "Cybersecurity" has come to mean a huge spectrum of things.[3] Not only does this lead to powers that are overly broad in scope and application,[4] but it also risks generating a consensus that is illusory. For example, the potential of cybersecurity threats to impact critical infrastructure does not transform the cybersecurity discussion into one focused primarily on threats to national security. Such threats, even if demonstrably tangible, will always remain one small part of the overall cybersecurity issue and should not be used to justify sweeping unaccountable powers. Further, without a clear understanding of what cybersecurity seeks to protect, it is impossible to develop tangible risk models and, by extension, to determine whether any resulting gains in security are proportional to any resulting impact on the rights of citizens. Powers that may be proportional when tailored to address national security concerns might not be as proportionate when employed in defense of private rights.

Absent specifics on risk assessments, the factual scope of the problem, and the "cybersecurity" rubric itself, it is difficult to speak of specific goals and objectives. However, it is possible to foresee challenges at a more general level relating to the need for proportional solutions that impact minimally on fundamental rights of citizens. There is an unfortunate tendency to re-couch cybersecurity issues in terms of "warfare" and "national security". While some aspects of cybersecurity might implicate these more serious concerns, conflating all cybersecurity issues in this way is not conducive to balanced policy-making. It can lead to the adoption of drastic solutions such as

network monitoring, despite the ready availability of more practical options that are respectful of citizens" rights.

Defensive "target hardening" is, generally speaking, a more effective solution to these cybersecurity problems. Target hardening requires addressing a host of problems, including insufficient access control, lack of encryption, poor network management, and failure to install security patches, inadequate audit procedures, and incomplete or ineffective information security programs. Ensuring proper incentives are in place for vendors, service providers, and governments to adopt this type of target hardening may be the best mechanism for member states to achieve higher levels of security on the Internet.

The example of botnets is illustrative of how the policy-making process may get unbalanced: We can all agree that botnets are a problem, but are they more fundamentally a symptom of a bigger problem—insecure software? Does it make sense to expand ISP–level monitoring and promote dramatic countermeasures as a solution to botnets if the problem is more directly related to security errors in software such as Windows, Safari, or Android? Better computer-based security solutions installed by default may do far more to address botnets then ISP policing. If this is the case, than the latter should not be a viable option given its grave implications for online privacy and expression.

In conclusion, the primary challenge to balanced cybersecurity policy-making and governance on the basis of informed multi-stakeholder discussions is the lack of clear priorities premised on a solid evidentiary basis an aimed at addressing specific and tangible harms. Current cybersecurity strategies lack specificity and grounding in demonstrable risk. It is critical for Members to enrich the public record by providing more details on the scope, nature, and dimensions of existing cybersecurity risks. Without this data, it becomes difficult to adequately assess proposals for their effectiveness and to ensure their impact on fundamental citizens' rights will be proportionate, or to determine whether less intrusive alternatives exist. Generally speaking, defensive target hardening is preferable to dramatic expansions of powers aimed at implementing monolithic "offensive" strategies. The latter often fail to address real security problems and can actually make matters worse by weakening existing privacy safeguards, disrupting the reliable operation of networks that are the subject of protection. Simpler practical measures that create real security by encouraging better computer hygiene are not only less intrusive, but in many instances they will be far more effective.

Response from ITAC

Preliminary comments

There is no consensus on what the term "cybersecurity" means. A lack of a common shared understanding of this term is the primary obstacle to the development of internationally compatible solutions. There also appear to be different views as to what falls within the scope of "national" vs. "private" cybersecurity.

National cybersecurity strategies appear to be heavily influenced by one of two starting point assumptions, i.e. whether governments regard the Internet as a fundamentally "trusted space" or an inherently "distrusted space".

Any discussion on "cybersecurity" needs to clarify and clearly articulate what is within scope. Is the objective to secure any or all of the following: devices connected to the Internet; the Internet infrastructure; applications; communications; data; identity; and/or "essential services" (e.g. electricity distribution) dependent on the Internet? The policy considerations are likely to be different in each of these cases.

In the end, a process which draws upon the interests and expertise of a broad set of stakeholders may be the surest path to success. For example, the development of robust inter-domain policies related to "cybersecurity" will need to address issues of control and compliance. Compliance programs that build and verify assertions may be one means to provide an approach with the ability to scale based on application in one or multiple jurisdictions and across business verticals. Compliance programs have the potential to move the discussion to a slightly broader base, which encompasses technology, policy, and operations.

Response to question 1

A key priority for the Internet technical community is developing technical security solutions that remain consistent with the fundamental properties of the Internet – global, open and interoperable, and communicating those solutions in ways that are understandable to policy and commercial decision-makers.

A key priority for society and the economy is to have confidence in the network. To be trusted, the Internet must provide channels for secure, reliable, private, communication between entities, which can be clearly authenticated in a mutually understood manner. The mechanisms that provide this level of assurance must support both the end-to-end nature of

Internet architecture and reasonable means for entities to manage and protect their own identity details.

Priorities (and challenges) include:

- Preserving the openness and global nature of the Internet, as well as its innovative potential, and fundamental human rights
- Finding the right balance between the various factors that enable trust and allow communications between end-users (i.e. reachability) such as security, privacy, reliability, resilience and usability
- Finding the right balance between security and an enabling environment for communication, trade, innovation and growth
- Recognising that different security solutions are needed for different types of interactions on the Internet and that the highest level of security attainable may not be the optimal solution in all circumstances
- Developing new solutions, critically assessing existing approaches and discarding old security paradigms that are not well suited to the Internet
- Realising that the implementation of security solutions is a long-term investment in the Internet ecosystem that everyone benefits from, and that stakeholders have a shared interest in the management of these resources

Cyber threats change rapidly making a mandatory, compliance-driven regulatory model ineffective and counterproductive by limiting needed flexibility to adjust to new threats.

The global nature of the Internet, communications networks and the ICT industry requires a global approach to address cybersecurity concerns. This global approach needs to be inherently based on multistakeholder collaboration and cooperation.

Any approaches to cybersecurity that increase technical barriers to trade in ICT infrastructure equipment and end user devices risk balkanising the global Internet into different markets with different technical regulations. This in turn would harm the global economies of scale, which have enabled the rapid deployment of broadband infrastructure. Furthermore, such approaches could create interoperability issues between countries and harm the growth of global ICT and other services.

2) What is the role and responsibility of governments with respect to public policy for cybersecurity? What do you see as the most important evolutions in government strategies?

Response from BIAC

In general, governments should recognise cyber-security as a growing challenge and should consider cyber threats as a matter of national security. More economic funds should be allocated in order to promote the collaboration of industries in realising national security infrastructure, aimed to identify and mitigate security threats.

Governments should also create more awareness on security topics by introducing for example security requirements into their call announcements for public sector services.

Governments of course have competence in making decisions of national security. Issues of civil liberties and how to implement policies appropriately and with as limited a burden as possible are topics that benefit from multi-stakeholder consultation. That being said, the divide between national security and economic security, where many more shared interests are at play, is ever more blurred. Furthermore, greater amounts of critical infrastructure are under the control of the private sector. Governments must thus find the appropriate balance between exercising their competence in national security and addressing issues that impact economic security and private sector systems. Increased cooperation and collaboration is developing in these areas, but more needs to be done.

Governments have the responsibility to take actions in the legal/regulatory field to improve, clarify, and enforce national laws in terms of cyber-crime. In this context they also have the role to promote the interoperability across the legal frameworks adopted by other countries. The cooperation between security agencies is essential because the jurisdictions have territorial boundaries that cyberspace has not. It is difficult to attribute responsibility, both for the difficulty to trace cyber events and for the lack of reference paradigms for a clear assignment of liability.

We believe that governments can play a key role in a closer interaction and cooperation between public and private sectors to combat cyber-crime. Cooperation between the private sector (such as universities, industries, associations, ISP, etc.) and government institutions is important to raise awareness to the cyber security issue and to ensure the resilience of critical infrastructure and the availability of the services.

In this way it is possible to implement an effective IT governance policy in terms of tools and resources necessary for the operation of networks and their resilience, and in terms of coordination mechanisms in case of security attacks on a large scale.

This co-operation can be more effective if it involves also international partners.

The OECD played an important role in related issues of cryptography years back where it was finally decided that security would be enhanced overall if companies were more broadly allowed to use cryptography which had been previously controlled in the manner of a munitions. Similar concepts must be at play today. While OECD member countries can do more in this area, the issue is especially relevant in many developing countries that have not had the same experience curve. The OECD and Member Countries have a significant role to play in outreach here. With global interference among systems and value chains governments can no longer just address security within their borders. Third countries may develop one off requirements that may intentionally or inadvertently compromise overall security. Only through the reinforcement of the need to rely on internally accepted standards can such outlier action be addressed. Obviously where OECD members' governments take similar national and unilateral action the ability to address global players on the issue is vastly diminished.

As was noted above, issues of security are global and multisectoral, thus one improvement noted in the OECD paper which should be further enhanced is the interdisciplinary work on security both across agencies within governments and across local as well as national governments.

In considering enhanced working relationships with the private sector, two areas of consultation should be prioritised:

- First, as prevention is fundamental, a better use of Computer Emergency Response Teams (CERT). Governments can promote the institution of CERTs and encourage the involvements of University and other corporations for information sharing and education strategies.
- Second, a greater consultation on the level, specificity and nature of guidance and law is needed. In many cases the level of specificity or proscription may not benefit security and may create significant and unintended burdens and consequences. Appropriate consultation can help ensure effective solutions that do not create such burdens or consequences.

Response from CSISAC

Governments must recognise that rivalries among nation-states constitute one of the chief security threats on the Internet. They can fund and provide the market demand for exploits and threats, which can then proliferate into the civilian economy. Taking advantage of zero-day exploits and the use of malware is highly questionable on practical and ethical grounds, and such activities do not lose their ethical murkiness when wielded by Governments.[5] Their geopolitical rivalries and development of offensive cyberwar capabilities can threaten the cooperative basis of international digital communications. Offensive cyberwar capabilities should be banned, or formally discouraged and limited if that is not possible. Also, governments need to formally recognise that their own massive data collection and surveillance efforts can, when breached, pose a threat to civilians and even to the very security concerns such surveillance seek to alleviate. Domestic efforts to survey citizens can like-wise lead to weakened security.[6] Governments should avoid imposing design obligations that undermine security in the name of their own surveillance efforts.

Governments must be cautious of knee-jerk reactions to perceived cybersecurity threats. Furthermore, they should collect rigorous evidence on such threats from an unbiased, independent source (e.g. not relying solely upon evidence from the cybersecurity industry) and should develop the capacity to generate their own measurements and to conduct their own assessments. Only through a more thorough understanding of the status quo can we begin to assess the incentives that produce problems and to address how to best correct them. A core element of this information-generating imperative is the need to implement breach notification obligations. Absent such obligations, it becomes difficult to begin to assess the scope of the problem, as many cybersecurity breaches will simply go unreported. We note further that breach notification obligations have also been recognised as a strong mechanism for instilling target hardening incentives.[7] An effective breach notification obligation will be two-tiered, with one lower standard controlling disclosure to a government authority for recording and oversight purposes, and a second, higher standard controlling disclosure to directly affected individuals.[8]

Governments have an obligation to ensure that any cybersecurity policies or strategies adopted are demonstrably necessary, fact-based, consistent with fundamental rights of citizens and proportionate to a legitimate aim.

Governments must lead by example. Defensive target hardening can address many of the most comprehensive and widespread cybersecurity issues. Vulnerabilities still abound, and incentives to prevent them are not firmly in place. Such security problems are shared by governments, the private

sector, NGOs, and individuals, and thus present similar problems and solutions. We all use the same computers, networking hardware, Internet protocols and software packages, which have the same vulnerabilities and problems. Governments can take the lead by implementing rigorous policies, technical tools and even legislative obligations to secure information systems and software for everyone as soon as vulnerabilities are discovered, while securing government operated infrastructure that relies on those systems. It is vital that government are committed to protecting software in general, and that patches to vulnerabilities are made available not only selectively for government targets, but also to the general public as well. Only with such a defensively oriented security culture will governments maximise safety for everyone.

By taking the lead, Governments will not only take great steps towards securing information of citizens and Government services, but will also generate policies and tools that others can use to similarly secure their systems. Government initiatives to secure internal networks can also provide a valuable source of information on what works and does not work, which can in turn form the basis of future policy discussions as well as government-led education campaigns. Such initiatives can also result in the identification and dissemination of information regarding threat metrics and dimensions – another area where Governments should be taking the lead. Governments are often the largest single domestic users of IT services, and have access to immense stores of valuable information that can be used to better assess cybersecurity issues. Mechanisms should be explored to make this information available on a regular basis.

Response from ITAC

A very significant evolution in government strategies has been the adoption of the multistakeholder model for policy development.

The drive towards more robust evidence-based policy decision-making led by the OECD (and others) is also very important.

The role and responsibility of governments is to foster the open, transparent and collaborative development and deployment of security solutions, and to develop policies in an actively engaged multistakeholder process.

It is important that governments do not adopt strategies that are reactive, but rather, develop an approach to cybersecurity that embraces technology and innovation, while protecting end-users and critical infrastructure.

Further, in forming public policies for cybersecurity, governments should be mindful that in some countries much of the critical infrastructure for telecommunications and the Internet is operated by non-governmental

entities, i.e. private entities, which bear the primary responsibility for securing their own networks and facilities.

As a mandatory regulatory model is unlikely be effective in addressing evolving cyber threats, government has a critical role to play in the leadership and coordination of cybersecurity efforts through legal reforms and public-private partnerships to facilitate information sharing and voluntary industry adoption of best practices. Governments can also show leadership through their own well-designed, balanced and judiciously applied trust compliance programs and procurement practices.

Finally, multi-stakeholder cooperation and leadership by governments should include:

- Co-operation and mutual assistance to ensure functionality of infrastructure and services before, during and after attack;
- Cooperation and mutual assistance to build more robust systems and networks;
- Leadership by governments to drive the market towards increasingly robust and resilient solutions;
- Governments encouraging the deployment of more secure solutions that preserve the fundamental principles of the open Internet.

3) How should governments implement cybersecurity policy at national and at international levels and how does this compare with current new strategies?

Response from BIAC

Governments should implement cybersecurity policy at national level having in mind the evolving and sophisticated security threats scenario and also taking into account the nature of the cybercrime which is not confined inside a single nation.

At international level it's necessary to share and coordinate with other countries on the development of global policies, addressing legal and regulatory requirements and sharing technical mechanisms and best practices to improve also interoperability. Strategies should promote cooperation at international level, reinforcing alliances and promoting incident response coordination.

Companies that create and deliver technology and services, as well as those that rely on technology and services to deliver critical infrastructure functions address security at the system and process level. Companies are

increasingly global and, as a result, they embrace international standards. Thus a global coherence or interoperability across national government policies is essential. Obviously that also has to apply to subnational government elements. We recognise that government may have national priorities that differ and may emphasise different aspects of security as more or less critical. These variances in approach should still allow for the deployment of global, coherent and cost-effective industry solutions.

As we consider the recent economic upheavals, we must be able to be as efficient as possible in the use of resources and deployment of technology. Needless or redundant documentation or proof/certification of systems leads to waste. The system used by the Common Criteria where evaluations done to a common set of standards by certified labs are globally accepted by participating countries optimises the use of costly resources. Such credible mutual recognition agreements create global benefit and avoid waste. Further exploration should also be undertaken to cross recognise compliance; systems that are found to be compliant with one set of regulatory requirements should be recognised as being found compliant with similar requirements for a different regulation. This is also consistent with a services oriented architecture approach, where, for example, an authentication service may be used across a number of solutions.

Response from CSISAC

As a starting point, it should be recognised that positive cybersecurity outcomes might not require dramatic legal changes. Rather, technical and governance solutions may go far to address many potential cybersecurity issues. As noted above, there has been a tendency to enact overly aggressive legislative measures where practical, technical solutions could yield much more effective results.

As also noted above, Governments must be more accountable and transparent about current and planned cybersecurity strategies, especially in approach to disclosing security vulnerabilities. This is crucial to democratic governance, trust, and good security. The culture of secrecy that permeates intelligence agencies fits poorly with best practices for private-sector civilian security and more generally, principles of multi-stakeholder Internet governance. More creative solutions to information sharing must be explored and, as a starting point, a strong presumption of maximum disclosure (rebuttable on a concrete basis) should be adopted as a guiding principle. Where a concrete basis for hiding information exists, it should not be withheld longer than is necessary.

Governments should ensure the implementation of cybersecurity policies at the national and international level in accordance with the 2002 OECD Security Guidelines. This means that measures taken to secure information systems and networks should be respectful of fundamental rights and democratic values, and premised on risk assessments. Governments should publish these risk assessments subject to the provisions noted above. Impact on privacy and civil liberties should be addressed explicitly in risk assessments. Similarly, Governments need to ensure that their own infrastructure is secure. They should do so holding particular regard to the protection of citizens' personal data and in keeping with OECD Privacy guidelines.[9]

Governments should be wary of large, monolithic cybersecurity projects that fail to address specific problems in a concrete and targeted manner. These suggest sweeping, unnecessary powers that are not justifiable. Instead, a case-by-case approach is advisable, aimed at addressing specific problems as identified by risk assessments.

Governments should ensure that cybersecurity strategies are not implemented in a manner that is in fact detrimental to its stated objective. A key example is the deterrent effect many security-based provisions have had on security researchers, who often face legal threats from organisations wielding cybersecurity powers in order to avoid the potential embarrassment of a publicly disclosed breach in safeguards.[10] Governments should ensure such legal protections, if adopted, do not interfere with legitimate security research and should audit existing protections to ensure legitimate research of this type is unhindered.

Response from ITAC

At the national level, cybersecurity policies should be developed and implemented in close collaboration with all interested and potentially affected parties in a truly open, transparent and inclusive multistakeholder approach. Such policies should be based on reliable evidence, a solid technological foundation and a proper understanding as to how the Internet works. Such policies should foster the development of open standards and permission-less innovation for security solutions. They should avoid unilateral modifications to the global Internet standards and technologies – any changes should be done using the appropriate channels (*e.g.* IETF and W3C).

Technology will continue to evolve – this is consistent with a vibrant and dynamic global Internet economy. Cybersecurity policies should be flexible enough to allow technology to evolve and to be responsive enough to address new threats as they arise. Solutions need to be workable, implementable and scalable.

Governments have a role to play in encouraging the development of new business models as technology advances. Regulators need to be careful not to stifle growth by protecting older models which may be overtaken by innovation.

Efforts should be placed on cybersecurity strategies that target the source, rather than the user or the intermediary. Governments should be careful to avoid overly prescriptive approaches, which risk freezing security solutions and stifling innovations in technology and Internet use.

National cybersecurity strategies will need to be mindful of national cultures and values, yet compatible with international strategies and the global nature of the Internet.

Protection of children online is a very important shared objective. However, it is also important that that objective not be misused as a justification for cybersecurity measures that are contrary to an open Internet.

A coordinated multi-agency approach across government is a useful step forward. It would also be useful to consider whether the agencies themselves also remain appropriate for the new environment.

Given the transborder nature of the Internet, international cooperation is crucial for effective cybersecurity. At the international level, policies should stimulate the creation and use of common terminology/definitions, encourage sharing of best practices and facilitate the information exchange that is essential to combating cybercrime. It is also important for cybersecurity priorities to be translated into technical solutions that work with the fundamental principles of the Internet and not against them.

As in policy development, the Internet technical community should be viewed as an essential partner in the implementation of cybersecurity policies.

4) What is the role and responsibility of business and industry/civil society/Internet technical community with respect to cybersecurity public policy? How is this reflected in the new strategies?

Response from BIAC

Business, as innovator and developer of hardware, software and services, the owner and operator of many critical infrastructure systems and developer or provider of many government owned and operated systems has a very significant role to play. Business plays this role directly in their technology development and operational policies, cooperatively in collaborative policy development with governments and in appropriate multi-stakeholder settings and in a directed fashion when implementing solutions for governments.

A number of strategies have consultation mechanisms, but again we raise concerns on how to best differentiate across areas of economic and national security. The ability of governments to consult effectively with business in the context of national and economic security to assure that there is appropriate cooperation in attaining mutual and important public policy goals while assuring that undue burdens are not placed on business is an objective of many of the strategies that needs greater emphasis.

Industry can actively cooperate and collaborate in the formulation of government policies related to cybercrime: monitoring, investment, counter-measures, harmonisation of terminology, laws etc. In particular the most important contributions can be in:

- Defining security measures for emerging threats; in this contest the IT industry should continually innovate and invest in the development of its products and services. Being an innovative and dynamic sector with rapidly changing and evolving technologies, the industry can give an important value to the cybersecurity in addressing new and evolving threats.
- Continue to lead or collaborate as appropriate in developing globally accepted cybersecurity standards, best practices, and international assurance programs.
- Developing and utilising comprehensive risk management strategies and best practices to achieve and maintain trust in the cyber infra-structure.

In conclusion, the responsibility of industry is to lead and contribute to a range of significant public-private partnerships and government initiatives, including information sharing, analysis, training and emergency response with governments and industry peers.

Response from CSISAC

When it comes to cybersecurity, civil society is often excluded from the process of policy making.

First, the involvement and lobbying of security industries and law enforcement in the political decision-making process, with the increasing exclusion of the citizenry, is concerning and leads to opaque policy processes and the marginalisation of the democratic process. Strong military and intelligence interests compound this problem of democratic deficit, and generally conflict with multi-stakeholder principles.

What also concerns civil society is the growing tendency towards public-private partnerships on cybersecurity strategies, which seem modelled on traditional intelligence community policy-making approaches and not on Internet governance. These approaches reduce democratic accountability and are further concerning in that they rely on private action that is often outside the scope of constitutional protections aimed at checking the otherwise overwhelming prerogative of the state.

Although international cooperation on cybersecurity may be necessary, state-to-state interaction on these matters often exclude civil society with the result that civil society concerns are ignored.

In regards to participation and openness, Governments should ensure the proper participation of civil society in the cybersecurity policy development process so that civil society can effectively play its role in the governance process — namely, to ensure values such as openness, concerns of individuals, and the protection of privacy, free expression, association, and access to information are taken into account in policy outcomes.[11] Civil society can also actively engage in facilitating cooperation among existing security networks, while making the network's actions more transparent and accountable.

Response from ITAC

The private sector, civil society and the Internet technical community are important stakeholders and should be involved in the development and implementation of cybersecurity policies. Only a truly multistakeholder approach will allow local, national and international communities to find the right balance between policy requirements, technical soundness, and civil rights of citizens, while ensuring the innovative potential of the Internet.

The Internet technical community is in the best position to provide independent advice to policymakers on the potential intended and unintended consequences of policy decisions to the Internet and the way that it works. Policymakers should seek this advice as early as possible in their policy development process to avoid pursuing technologically flawed decisions.

The Internet technical community is also in a unique position to develop building block security solutions (e.g. SSL) that can be deployed by others to provide Internet users with various options and varying degrees of security in their Internet experience. Such building blocks can also be used to achieve national cybersecurity objectives (e.g. using DNSSEC to secure government email communications).

It should also be noted that the Internet technical community's work to improve the security of Internet infrastructure (occurring independently of national or international cybersecurity policies) is quietly supporting the overall policy objective of a more secure and trusted Internet. Fundamental to this is the Internet model of developing standards openly, collaboratively, and by consensus.

Examples of technical standards developed by the Internet Engineering Task Force (IETF) to improve the security of Internet infrastructure include:

- Secure BGP (Border Gateway Protocol)
- DNSSEC (Domain Name System Security Extensions) – securing integrity and authenticity of DNS responses
- RPKI (Resource Public Key Infrastructure) – an infrastructure to support certification of the Internet Number Resources and the foundation for the solutions of security of the global routing system
- Kerberos Network Authentication System – provides a means of verifying the identities of entities on an open (unprotected) network
- TLS (Transport Layer security) – provides communications security over the Internet
- IPsec (Internet Protocol Security) – provides the end-to-end security at the Internet layer

Examples of technical standards work under development and consideration at the World Wide Web Consortium (W3C) to improve the security of the Web and the Internet include:

- Content Security Policy
- Cross-Origin Resource Sharing
- XML Signature, XML Encryption and related specifications
- cryptographic APIs for JavaScript

Examples of OASIS data security standards include:

- Digital Signature Services (DSS) – digital signature services standards for XML
- Key Management Interoperability Protocol (KMIP) – provides extended functionality to asymmetric encrypted key technologies

- Security Assertion Markup Language (SAML) – XML-based framework for creating and exchanging security information between online partners
- eXtensible Access Control Markup Language (XACML) – representing and evaluating access control policies

Example of requirements and frameworks specifications from the ISO/IEC include:

- IS27001 – Information Security Management Systems – Requirements
- IS27002 – Code of Practice for Information Security Management
- DIS29115 – Entity Authentication Assurance Framework

An example of a trust framework from the Kantara Initiative is:

- Identity Assurance Framework – Service Assessment Criteria (IAF-SAC) – provides criteria for assessment of a Credential Service Provider (organisational, credential management and identity proofing)

The ICT industry is also working collaboratively through public-private partnerships to secure communications infrastructure. For example, in the US, in the Communications Sector Coordinating Council, the IT Sector Coordinating Council, CSRIC, NSTAC, NCCIC, ISACs among others. The industry is also developing voluntary security measures such as Safecode and OTTF. The telecommunications industry has incorporated security measures into technology-specific standards, such as 3GPP and 3GPP2.

The industry should work together with all stakeholders to further develop standard, unified privacy-respecting methods to collect, analyse and report data breaches at a global level to provide industry and government with a better understanding of, and ability to combat, cybersecurity threats.

5) What is -or what will be- the impact of recent cybersecurity strategies on business and industry/civil society/the Internet technical community?

Response from BIAC

Increased certainty and assurance will accrue to business and industry in the form of greater trust in the infrastructure and services and government adoption of new technologies helps demonstrate the capacity of and faith in technology.

That being said, technology mandates, prescriptive rules and detailed requirements are not usually appropriate vehicles for achieving government objectives. Government should work with non-government stakeholders to build better risk-based strategies that are agile enough to respond to rapid changes in the global threat environment.

Issues related to corporate and organisational policies dealing with security and supply/value chains need to address corporate realities and business needs. The desire to help assure security by government mandated specific or detailed requirements related to operations and supply chain may often constrain innovation, create burdens and increase costs without improving overall security. Similarly in some non-OECD countries, procurement or domestic preferences in the guise of security requirements or requirements related to security may either impair trade or otherwise skew a level playing field to the disadvantage of overall security by precluding or significantly hindering the ability of companies and organisations to roll out globally consistent processes and infrastructures.

Response from CSISAC

More mass surveillance policies, less accountability, and transparency

As mentioned above, there is a morally hazardous problem with current cybersecurity approaches that focus on "offensive" security measures (e.g. surveillance and countermeasures, combined with almost zero civil or criminal liability).[12] Incentives are being put in place that are seemingly calculated to encourage private-sector exercise of power that is sweeping, easy to hide/abuse, and effectively unchecked. Those are defective incentives. These open-ended immunity regimes are also indicative of the monolithic approach to cybersecurity warned against above.

Furthermore, it rarely seems that citizens and their needs are at the center of cybersecurity policies. Vulnerabilities faced by users and specific technical problems are usually not addressed, and instead the language is high-level, vague, and abstract. It is sometimes difficult to see what aspects, if any, of these policies are in the immediate interest of the general public. Some context-specific problems include:

Identity Management Schemes

One set of strategies being touted as a solution to the cyber security problem is to promote widespread identity management schemes, in which a user potentially has to authenticate to some system before a network (or some aspects of a network) is accessible to her. Even her low-level actions

such as the sending of packets may be attributable to her authenticated identity under some proposals. In addition to being a disruptive departure from the way the Internet works now, we should not assume that such authentication or identity management schemes would lead to good security. For one, implementation challenges would create a whole host of new vulnerabilities and security issues. Moreover, even setting these security issues aside, it is not certain that attribution would be all that useful. Regardless, there are benefits to preserving the capacity for online anonymity that far outweigh any potential alleviating effects an "identity infrastructure" could provide, even in the best case.

Chilling People's Freedom of Expression Rights

Specific tactics such as the "Internet kill switch" and communications shutdowns are particularly powerful in restraining speech and association. This kind of measure does not only operate in authoritarian regimes; indeed the Prime Minister of the United Kingdom, in the midst of civil unrest last year, proposed shutting down social networking sites and the Blackberry messaging service. Similar proposals have been voiced in the United States, only to be dismissed as impractical on a network level. Given the potential for misuse of such shutdown powers, they should be categorically avoided.

Finding a Proportionate Approach: Hacktivism and Online Protest

Governments have been targeting online political protesters — "hacktivists"— for actions directed at both states and corporations. There have been examples where the severity of activities conducted by such entities have been described as analogous to the threat posed by terrorist organisations and organised crime. Sometimes the supposed harm that results from an act of hacktivism — such as the temporary defacement of a website[13] — has a *de minimis* quality that belies its characterisation as a "cybersecurity threat". In other instances, acts of hacktivism have the potential to cause more serious harm if for example these were turned to denial or delay of access to essential services. In assessing the proportionality of responses to this type of conduct, it is important that these extremes are not conflated.

Politically motivated DDoS attacks and other forms of hacktivism can be both legitimate forms of protest and a violation of the rights of targeted sites. They can also threaten the public interest by, for example, hindering democratic participation.[14] The line between the two is not always clear. Whistleblowing and releases of classified information that expose governmental abuses also blur the line between legal and illegal activity. This kind of hacktivism, therefore, must always be assessed through the lens of

traditional civil and political rights and not conflated with "national security" threats or "cyberwarfare". Policy responses should be nuanced and recognise the intersection with free expression, political accountability, and legitimate protest. Specifically, cybersecurity strategies should not unduly and disproportionately interfere with important democratic activities such as collaboration, participation, coalition building, advocacy, fundraising, and the dissemination of information by individuals and groups.

Extra-Territorial Impact of Cybersecurity Policies

The cybersecurity strategies of one government can affect citizens of another country due to the cross-border nature of communications. Some of these strategies, however, can be very damaging for citizens of all countries involved. An example is the recent distribution of pro-government malware in Syria, which was released from within the country first onto satellite networks and set up in the absence of access to national infrastructure. The malware—targeted at Syrian opposition activists—later spread to users' computers outside of Syria, capturing webcam activity, disabling notification settings for certain antivirus programs, recording key strokes, stealing passwords, and sending this sensitive information to a Syrian IP address.[15] Thus, the extra-territorial effects of cybersecurity policies should also be taken into account by governments when they are formulating these policies, especially the impact on civil society activism work in other countries.

Response from ITAC

Cybersecurity policies, developed through open, consensus-based processes, could be a key element to the continued growth and robustness of the Internet. They could help facilitate online commerce, secure government networks, and enhance the online user experience. However, poorly crafted cybersecurity strategies could have the opposite impact. For example, cybersecurity approaches that emphasise hardening of networks or extensive government controls could result in network fragmentation, higher costs for providers and users of online services and applications, and stifle free expression. Cybersecurity approaches require a delicate balance of many interests, roles and responsibilities within the Internet ecosystem – we all have a role to play. Tilting the balance in one direction or the other will inevitably have broad impacts at the local, national and international level.

6) How should national cybersecurity strategies and policies be evaluated? What metrics should be applied to measure their efficiency?

Response from BIAC

To be efficient national cybersecurity strategies and policies should be periodically evaluated and updated so that improvements can be implemented to face new security threats. This can be performed by:

- A periodic comparison with strategies and policies of other countries.
- Producing periodic country reports to share information about security incidents and the level of damages created.
- Planning recurrent cybersecurity risk assessments to verify the efficacy of the security measures applied. This output could be used to review the cybersecurity strategies and policies.
- Capacity building to ensure that the needs of less advanced companies and small and medium sized firms are also addressed.

While it would be nice to be able to comparatively evaluate cybersecurity strategies, the paper indicates that each national strategy has its own definitions, priorities and implementation methods suited to the legal and cultural context of the nation. It would thus be best to measure the effectiveness of such strategies within the national deployment and then separately measure how well the strategies enabled cooperative work across jurisdictions.

While the topics and implementation methodologies vary, there could be some uniformity in the measurement criteria that could further enable some levels of comparison or at least create some referencable bench marks. It should be noted that cost-effectiveness, useful information sharing, complaints, positive or negatives impacts on the level of security as measured by breach or other malicious behaviour, costs to business and attributable growth in the usage of the internet and the economy could all be useful metrics.

Response from CSISAC

National cybersecurity policies must be evaluated by their impact on fundamental rights and legitimate considerations of citizens as set out in Principles 4 and 5 of the 2002 Security Guidelines. A successful cybersecurity strategy will ensure that, prior to its adoption, each specific cybersecurity initiative it envisions is designed in a manner consistent with core

values recognised by democratic societies, such as freedom of expression, privacy, due process, and transparency. The effectiveness of each cybersecurity proposal should be measured by these metrics and consistent with fundamental human rights. A human rights compliance checklist or Impact Assessment should be a mandatory element of the assessment process for each cybersecurity initiative. Further, any impact on fundamental rights must be narrowly tailored to address a specific, well-defined cybersecurity threat that presents a demonstrable risk of tangible harm. In recognition of the ever-shifting technological landscape that characterises the Internet, there is a risk that cybersecurity initiatives, even if proportionate when initially adopted, may grow to impact significantly on fundamental rights as technology evolves. Cybersecurity strategies should therefore build in 5 year sunset clauses or mandatory rights impact assessment reviews to ensure adopted policies do not grow over time in a manner that is inconsistent with fundamental rights.

Ultimately, the policy debate must be done transparently and in public. This is an area where opacity is produced not only by withholding information from the public (on grounds that it would compromise company secrets or alert criminals to vulnerabilities) but also through the prevalence of discussions and legislative proposals so broad and vague it becomes impossible to know what powers are actually being granted and the purposes for which they will be used.[16] Monolithic solutions of this nature are not only problematic because they tend to be broader than the issues they are designed to address, but also in that they effectively immunise the use of such powers from proper assessment of their effectiveness, proportionality, and impact on fundamental rights. It is difficult to gauge the scope, intended use and effectiveness of cybersecurity powers premised on a vague need to produce "a general increase in cyber insecurity" or, alternatively, of powers aimed at enhancing national security, but which are open-ended in the conditions under which they might be used.

Response from ITAC

No cybersecurity policy will be able to address 100% of all online risks. Further, there will not be a "one size fits all" policy that is appropriate for all instances. However, these are some baselines considerations (*this is not an exhaustive list):

- Is the policy developed with an open, inclusive and transparent process?
- Does the policy approach encourage and support global interoperability?

- Is the policy approach flexible enough to address the changing online environment?
- Does the cybersecurity strategy protect basic human rights such as freedom of expression and provide adequate privacy protection for end-users?
- Does the policy create an environment of information sharing?
- Are the roles and responsibilities of the various stakeholders well understood and respected through the policy?
- Does the policy support appropriate voluntary adoption of globally developed standards and best practices to address cybersecurity threats?
- By what means is compliance with policies proven – fostering trust in actors that policies are actually being acted upon by government and private organisations?

One metric for the effectiveness of policies would be to measure the level of international participation pre- and post- policy implementation. A successful set of policies should increase Internet users willingness to access Internet services and systems, and would increase their overall willingness to participate in the ecosystem. Internet users may never understand many of the issues surrounding cybersecurity policies, however many users have the ability to "vote with their feet" regarding the use of services and participation in Internet communities at the local, national and international levels.

Another way to look at efficiency is to consider the collateral consequences and cost of a policy.

Notes

1. See "Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems". Katitza Rodriguez and Marcia Hoffman, EFF, 2011. Available at *www.eff.org/sites/default/files/filenode/Submission-Parliament-Hacking-Tools-vf.pdf*. and "Facebook Inc. v. Power Ventures, Inc., Case No. C 08-05780 JW (N.Dist. Calif., 2012); Sony LLC v. Hotz, Case 3:11-cv00167-SI, (Dist. Calif., 2011).

2. See "Dangerously Vague Cybersecurity Legislation Threatens Civil Liberties", Dan Auerbach and Lee Tien, EFF, 2012. Available at *www.eff.org/deeplinks/2012/03/dangerously-vague-cybersecurity-legislation*.

3. Various proposed U.S. legislative initiatives, for example, adopt extremely vague or broad definitions of cybersecurity threats that can include, in some instances, 'theft or misappropriation of private or government information, intellectual property, or personally identifiable information'. This provision will allow ISPs to monitor communications of subscribers for potential intellectual property infringements; block accounts believed to be used in infringing; block access to websites such as The Pirate Bay believed to be carrying infringing content; or take other measures provided ISPs claim it was motivated by cybersecurity concerns. Also, of concern is the language of "theft or misappropriation of private or government information" in some bills, which might be used to block sites such as WikiLeaks and the New York Times which have published information deemed classified.
   See *www.eff.org/deeplinks/2012/03/rogers-'cybersecurity'-bill-broad-enough-use-against-wikileaks-and-pirate-bay*.

4. See "Dangerously Vague Cybersecurity Legislation Threatens Civil Liberties", Dan Auerbach and Lee Tien, EFF, 2012. Available at www.eff.org/deeplinks/2012/03/dangerously-vague-cybersecurity-legislation.

5. "Wikileaks docs reveal that governments use malware for surveillance", Ryan Paul. Ars Technica, 2012. Available at *http://arstechnica.com/business/news/2011/12/wikileaks-docs-reveal-that-governments-use-malware-for-surveillance.ars*.

6 . "The Athens Affair", V. Prevelakis & D. Spinellis, 44(7) *IEEE Spectrum* 26 (2007). Available at *http://spectrum.ieee.org/telecom/security/the-athens-affair*.

7 . "The Evolving Privacy Landscape: 30 Years After the OECD Guidelines", OECD, 2011, p. 31. Available at *www.oecd.org/internet/interneteconomy/47683378.pdf*.

8. CSISAC notes that breach notification obligations are currently being discussed within the context of updates to the OECD Guidelines on the Protection of Privacy and Transborder Flows.

9. Paragraph 4 of the Guidelines requires that Exceptions to the Principles contained therein, "including those relating to national sovereignty, national security and public policy ("public order")" should be as few as possible.

10. There are many examples in the US of instances where security researches have faced legal threats under anti-hacking provisions found in the CFAA as well as under analogous anti-circumvention protection measures found in the US DMCA. See *www.eff.org/sites/default/files/eff-unintended-consequences-12-years_0.pdf*.

11. "Towards a cyber security strategy for global civil society?", Ron Deibert, Global Information Society Watch. 2012. Available at *www.giswatch.org/sites/default/files/gisw_-_towards_a_cyber_security_strategy.pdf*.

12. See a broad set of provisions aiming at providing unlimited civil and criminal immunity in US (see www.eff.org/deeplinks/2011/11/house-committee-rushing-approve-dangerous-information-sharing-bill) and Canadian legislative initiatives, for example (see *www.cippic.ca/sites/default/files/20110809-LT_Harper-Re_LawfulAccess-FINAL.pdf*).

13. "Apparently hacked, Syrian government website condemns president", Ahmed, CNNWorld, 8 August 2011. Available at *www.cnn.com/2011/WORLD/meast/08/08/syria.ministry.site.hacked*. Bruce Schneier compares the "harm" caused by some DDoS attacks to the service delays caused by a crowd of protestors standing in front of a service outlet: Schneier compared the pro-WikiLeaks attacks on MasterCard and Visa to a bunch of protesters standing in front of an

office building, refusing to let workers in. It's annoying, but it didn't shut down the operation. And it didn't start a war. "Is Wikileaks Engaged in 'Cyber war", J.D. Sutter, CNN Tech, 9 December 2010. Available at *http://articles.cnn.com/2010-12-09/tech/wikileaks.cyber.attacks_1_cyber-war-cyber-weapons-cyber-attacks/2*.

14. See for example this case study in zero day voter suppression and electronic miss-information campaigns in "E-Deceptive Campaign Practices Report 2010: Internet Technology & Democracy 2.0", EPIC, 2010. Available at *http://epic.org/privacy/voting/E_Deceptive_Report_10_2010.pdf*.

15. "How to Find and Protect Yourself Against the Pro-Syrian-Government Malware on Your Computer". Eva Galperin, EFF, 2012. Available at *www.eff.org/deeplinks/2012/03/how-find-syrian-government-malware-your-computer-and-remove-it*.

16. Examples can be found in recent U.S. cybersecurity legislative initiatives. See "House Committee Rushing to Approve Dangerous "Information Sharing" Bill". Kevin Bankston, EFF, 2011. Available at *www.eff.org/deeplinks/2011/11/house-committee-rushing-approve-dangerous-information-sharing-bill*.