OECD publishing

Please cite this paper as:

OECD (2012), "Non-governmental Perspectives on a New Generation of National Cybersecurity Strategies", *OECD Digital Economy Papers*, No. 212, OECD Publishing, Paris.
http://dx.doi.org/10.1787/5k8zq92sx138-en

OECD Digital Economy Papers No. 212

Non-governmental Perspectives on a New Generation of National Cybersecurity Strategies

OECD

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

16-Nov-2012

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

Working Party on Information Security and Privacy

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

Contributions from BIAC, CSISAC and ITAC

JT03330865

DSTI/ICCP/REG(2012)7
Unclassified
English - Or. English

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 cybersecurity 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 countermeasures 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 antivirus 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 cybercriminals 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 coordinated 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

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).

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

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.

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 cooperation 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 surveille 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

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.

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.

---

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.

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:

- Cooperation 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.

---

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.

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 freesing 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 infrastructure.

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 modeled 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:

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.

- 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

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).

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.

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.

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

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.

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 behavior, 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?

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.

- 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.