Moving Forward Together:
Recommended Industry and Government Approaches for the Continued Growth and Security of Cyberspace

Presented at the Seoul Conference on Cyberspace 2013

Authored by

BSA | The Software Alliance

DIGITALEUROPE

Information Technology Industry Council

Japan Electronics and Information Technology Industries Association

Korea Internet Corporations Association

The shared, interconnected nature of cyberspace creates opportunities and challenges. While technologies and services are overwhelmingly used for positive purposes, as with almost every aspect of society, they can be misused, abused, or exploited. Technologies and services change and evolve rapidly, and policymaking related to cyberspace must also be innovative to support growth, security, trust and confidence, and stability. This paper outlines approaches industry and government should advance to support the continued growth and benefits of cyberspace in the face of evolving challenges.

Introduction

The economic, social, and cultural benefits of cyberspace to citizens, businesses, and governments are far-reaching. Information and communications technologies and services (ICTs) have enabled innovations that advance society, spur economic opportunity and growth, and connect people across the globe in new and meaningful ways.

The shared, interconnected nature of cyberspace, however, also creates challenges. While ICTs are overwhelmingly used for positive purposes, as with almost every aspect of society, ICTs can be misused, abused, or exploited by some. All stakeholders—governments, industry, academia, and civil society—contribute to the development of cyberspace, and all have important roles in continuing to promote its growth and addressing challenges that could impede progress. We commend the Government of Korea's organization and sponsorship of the Seoul Conference on Cyberspace for bringing together thought leaders from governments, international and regional organizations, non-governmental organizations, academia, and industry to explore some of the challenges and opportunities presented by cyberspace and their accompanying policy questions.

Technologies and services change and evolve rapidly, and policymaking related to cyberspace must also be innovative to support growth, security, trust and confidence, and stability. An open, inclusive, light-touch policy framework facilitates the invention, diffusion, and uptake of new technologies, and enables countless new ideas, business models, and opportunities around the world. Government, industry, academia, and civil society must sustain and build on that approach as we address emerging challenges by collaborating and innovating to create globally compatible policies to universal challenges so that the economic, societal, and cultural benefits of cyberspace can be fully realized.

Industry appreciates the opportunity to engage with all stakeholders and contribute to the ongoing, global dialogue on cyberspace policy. This paper offers our thoughts on approaches industry and government should advance that will support the continued growth and benefits generated by cyberspace in the face of evolving challenges. While our recommendations focus on the roles of industry and government, we appreciate and look forward to meaningful discussion and collaboration with the variety of important stakeholders contributing to this effort.

1) Economic Growth and Development

The ICT sector has contributed to significant economic growth and development since commercialization of the Internet in the late 1990s. For example, global output from IT industries more than doubled from USD $1.2 trillion in 1995 to USD $2.8 trillion in 2010, accounting for 6% of global GDP.[1] ICT-intensive employment has grown steadily to make up over 20% of total employment in OECD countries.[2] Growth linked to the digital economy is contingent on policies that enable governments, businesses, and the public to access and adopt technologies and services.

Industry stakeholders should:

- Contribute to the development of globally recognized, industry-led, voluntary consensus security standards, best practices, assurance programs, and conformity assessment schemes.
- Protect and respect consumers' rights online in accordance with local laws.

Government stakeholders should:

- Adopt open, light-touch policy frameworks that promote the invention, diffusion, and uptake of new technologies, including broadband, mobile, and cloud computing platforms.
- Develop and maintain infrastructure that supports reliable access and use.
- Define policies, including trade policies, which provide access to and promote an interconnected, global market for ICT.
- Strive for laws and policies that are compatible on an international basis and mindful of international implications and reciprocity.
- Promote the rule of law and the adoption of laws, policies, and practices that protect intellectual property.
- Direct development aid toward the development of enabling ICTs.

2) Social and Cultural Benefits

The social and cultural benefits of cyberspace are far-reaching, from providing children in developing countries with access to educational tools previously unavailable, to helping rural farmers to access current crop prices and microbusinesses to sell their wares around the globe. The benefits of access to information and services, increased participation in the policymaking process, and greater understanding and appreciation for others has a profound impact on society.

Industry stakeholders should:

- Continue to support digital literacy with training and resources.
- Contribute training and resources for disaster and humanitarian response.

Government stakeholders should:

- Leverage ICT to deliver and enhance government information and services for citizens (i.e., support e-government).
- Support education and training to create highly skilled workforces.
- Define policies that enable markets to attract and hire the best talent from the global talent pool.
- Promote the free flow of online information across borders.

---

[1] National Science Board (United States), *Science and Engineering Indicators 2012*, January 2012, 6-15, at http://www.nsf.gov/statistics/seind10/pdf/c06.pdf

[2] OECD Information Technology Outlook 2010, http://www.oecd.org/internet/ieconomy/oecdinformationtechnologyoutlook2010.htm

3) Cybersecurity

The benefits of cyberspace are far reaching, but the risks associated with malicious activity must be managed in an ongoing fashion. Effective approaches to prevent, detect, and respond to cybersecurity threats require policies that meet security needs while preserving interoperability, openness, and a global market for ICTs. By partnering effectively, focusing on outcomes, and leveraging global standards, security can be enhanced without significantly hindering the economic or societal benefits of cyberspace.

Industry stakeholders should:

- Work to build and maintain security of technologies and services, including coordinating vulnerabilities and responding to incidents in a manner that reduces risks.
- Participate in public-private partnerships that enable all stakeholders to better manage cybersecurity risk.
- Contribute to the development of globally recognized, industry-led, voluntary consensus security standards, best practices, assurance programs, and conformity assessment schemes.

Government stakeholders should:

- Develop and implement cybersecurity policies in a transparent manner and with relevant stakeholder input.
- Encourage the development and use of globally recognized, industry-led, voluntary consensus security standards, best practices, assurance programs, and conformity assessment schemes.
- Promote market-driven technology innovation.
- Invest in security-related research and development (R&D) to support and complement industry efforts.
- Leverage existing cooperative incident response forums such as the Forum of Incident Response and Security Teams (FIRST).
- Raise awareness and education about basic cybersecurity hygiene.

4) International Security

The risks to and benefits from cyberspace are shared across the global user community. Because cyberspace offers a unique global commons, cooperation among global players is paramount to advancing social, economic, and cultural goals while addressing security-related imperatives.

Industry stakeholders should:

- When requested, provide views on technical considerations and likely implications on industry of international cyberspace security policies discussed in intergovernmental fora.

Government stakeholders should:

- Develop national and international strategies and agreements to advance security and stability of cyberspace, prevent unintended escalation of future conflicts regionally and internationally, and resolve cyber conflicts through reliable and peaceful methods.
- Be as transparent as possible to increase confidence and predictability in cyberspace.
- Engage with industry to inform development of policies.

5) Cybercrime

Cyberspace, with its global connectivity, poses considerable challenges to those tasked with enforcing criminal laws where they exist. The innovation in criminal activity and the distributed nature of bad actors can make enforcement and response very challenging. However, we must acknowledge the analogies between the off-line and on-line worlds. These are traditional actors and crimes - the difference is the medium - and there are traditional laws and government bodies that have long been tasked with dealing with them.

Industry stakeholders should:

- Strive to manage and mitigate risks to their own networks, products, and services.
- Utilize various methods to deter cyber threats such as training employees to understand techniques used by bad actors, and implementing tools to identify untrusted and improper behavior on networks and taking appropriate action.
- Cooperate with lawful requests for information and promote greater transparency about lawful access.
- Cooperate with governments in efforts to identify and prosecute online criminals.

Government stakeholders should:

- Update criminal statutes to clarify and enhance law enforcement's ability to prosecute truly bad actors.
- Increase law enforcement resources to combat cybercrime and enhance international assistance and engagement efforts related to cybercrime enforcement.
- Adopt legislation that addresses cyber crime by aligning with international approaches, improving investigative techniques, and increasing cooperation among nations.

6) Capacity Building

A fundamental aspect of advancing the benefits of and managing the risks in cyberspace is capacity building at a global level. This should come in many forms including legal, technical, and policy capacity-building efforts. There are numerous examples of successful global efforts to build capacity on ICT issues across the globe, and industry, civil society, and governments should work in partnership to build capacity and build upon the work done by various organizations. For example, the World Bank's West Africa Regional Communications Infrastructure Program (WARCIP) seeks to bridge connectivity gaps between 16 West African countries and the rest of the world, while the ASEAN Broadband Corridor project aims at establishing areas in each ASEAN member state with high- speed Internet connectivity.

Industry stakeholders should:

- Listen to the needs of all relevant stakeholders.
- Develop capacity building programs that leverage the unique expertise of industry.
- Share case studies, best practices, and lessons learned on capacity building in cyberspace, including how industry has been effectively engaged.
- Participate in and contribute to regional and international fora to promote sharing of best practices, lessons learned, and international technical exchanges.
- Integrate cybersecurity into cyber capacity-building initiatives, as appropriate.

Government stakeholders should:

- Provide developing countries with guidance and solutions to integrating the Internet into their economies in a way that will lead to economic growth.
- Invest in building and strengthening their own capacity in areas such as e-government, e-health, and e-education.
- Develop and share knowledge, training, and other resources with other countries seeking to build capacity.
- Participate in and contribute to regional and international fora to promote sharing of best practices, lessons learned, and international technical exchanges.
- Integrate cybersecurity into cyber capacity-building initiatives, as appropriate.

About the Authors

BSA | The Software Alliance: BSA is the leading global advocate for the software industry. It is an association of world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life. Through international government relations, intellectual property enforcement, and educational activities, BSA expands the horizons of the digital world and builds trust and confidence in the new technologies driving it forward. www.bsa.org

DIGITALEUROPE: DIGITALEUROPE represents the digital technology industry in Europe. Our 100+ members include some of the world's largest IT, telecoms, and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit from digital technologies and for Europe to grow, attract, and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. www.digitaleurope.org

The Information Technology Industry Council (ITI): ITI is the premier advocacy and policy organization for the world's leading innovation companies. ITI navigates the constantly changing relationships between policymakers, companies, and non-governmental organizations, providing creative solutions that advance the development and use of technology around the world. www.itic.org

JEITA: The Japan Electronics and Information Technology Industries Association (JEITA) is a leading Japanese organization comprising around 400 enterprises with global operations in the IT electronics sector, including consumer electronics, industrial electronics, semiconductors, electronic components and software. The objective of JEITA is to promote the healthy manufacturing, international trade, and consumption of electronics products and components in order to contribute to the overall development of the electronics and information technology industries. www.jeita.or.jp

Korea Internet Corporations Association (KINTERNET): Representing nearly 200 members, KINTERNET is a leading organization dedicated to assisting domestic Internet enterprises realize a better business environment. KINTERNET promotes the use of the Internet in the private and public sectors, proposes policies for the improvement of the environment of Internet businesses, performs research, conducts international exchanges, and supports enterprises' management. KINTERNET cooperates with various government and economic organizations as we advance these goals. www.kinternet.org