

**Bringing governments,  
businesses and  
academia together  
against cyber threats.**



# Cyber Threats Cannot Be Fought Alone.

Cyber-security is, and must necessarily be, an area of concern for us all. We now live in a highly connected digital world, where every aspect of our daily lives from communications, public utilities, financial networks to national defence - and so much more, are highly dependent on Information and Communications Technology (ICT) to function. Nevertheless, as societies get more 'wired' and 'connected,' we also become more vulnerable. Sadly, the kind of threats that were once the exclusive domain of the real world are creeping their way into the cyber world. Just as there are malicious individuals and groups bent on causing harm to societies and nations in the real world, governments around the world must prepare to deal with similar threats in cyber-space.

Since cyber threats can strike from virtually anywhere in the world, governments cannot contain this threat by domestic measures alone. Neither should governments be left to grapple with this danger on their own any longer, as the expertise and skill to combat these threats are largely dispersed across the globe and in many cases found outside government hands in the private sector or academia.

Bridging this gap between domestic and international and public and private is the role IMPACT seeks to play in ensuring the protection and security of each government's cyberspaces and critical ICT infrastructures.

IMPACT stands as a world-class international organisation that will effectively enhance the capability of the global community to prevent, defend and respond to cyber threats. By providing a platform to stimulate cooperation between governments, as well as between governments and the private sector of the world, IMPACT provides the world's first truly international collaborative institution against cyber threats.

# Cyber Attack Cases Around The World

Some argue that targeted cyber attacks and acts of cyber terrorism may be over-sensationalised, but with real-life incidents such as these, we can no longer afford to ignore it.

A hacker just has to worm into an IT infrastructure, bypass firewalls, and plant a code that gives him remote access and control over the target computer systems to create mayhem.

With the range of tools available, these cyber-attacks can originate from as wide a scope as geeks who hack into computer systems for fun, to terrorists with a political agenda.

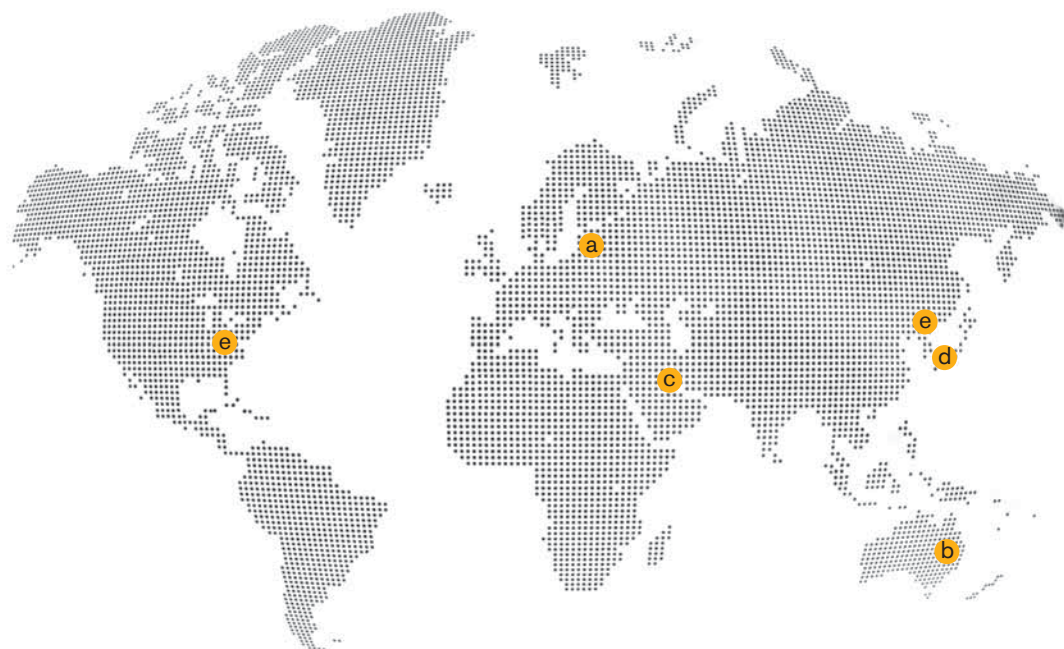
In the very recent past, cyber threats have become a grim reality, as these incidents prove:

## **a** Estonia

Estonia, one of Europe's most wired nations, found itself fighting the world's first cyber-war in 2007. Criminals bombarded the country's Internet servers until they crashed. The cyber attacks paralysed networks of the Estonian government, police, ministries, banks and media. To counter the attacks, Estonia was forced to disconnect from the Internet, causing large-scale disruption to its economy. Today, Estonia is in a leadership position in the fight against cyber-terrorism.

## **b** Australia

A disgruntled, unsuccessful job applicant to a waste management plant in Queensland sabotaged the plant's computerised sewage control system releasing millions of litres of raw, untreated sewage along Australia's Sunshine Coast, killing marine life, and spilling into local parks and rivers. In a separate incident in May 2008, a hacker hacked in and shut down several government databases in Darwin including servers for the Health Department, hospital, prison and Supreme Court, deleting the accounts of 10,475 public servants.



#### **c Persian Gulf**

Early in 2008, undersea communication cables were inexplicably cut. Sudden disruptions of Internet connectivity affected countries that included Egypt, United Arab Emirates, Saudi Arabia, Qatar, India, Pakistan and Bangladesh and chalked up millions of dollars in lost revenue. Damages to undersea cables are not uncommon. However, the vast extent of damage incurred in the recent incident underlines our dependence on Internet-based communications and transactions, and the need to defend against cyber threats.

#### **d Japan**

In Japan, some of the 24 million users of DoCoMo's i-mode mobile phones had their handsets taken over by a malicious programming code delivered by email. The code directed the phone to dial 110 - Japan's emergency hotline number. The mass numbers of phones dialling the emergency number caused the system to shut down.

#### **e USA and South Korea**

On July 4, 2009 a paralyzing barrage of electronic cyber attacks was unleashed upon government computers and networks in the US and South Korea, underscoring the growth in assaults against vital state infrastructure. It utilized a variety of well-known distributed denial of service (DDoS) attacks that try to overwhelm Web sites with useless requests and make them unavailable for legitimate users.



# Join the Forces of IMPACT.

IMPACT, the International Multilateral Partnership Against Cyber Threats, is the first global public-private initiative against cyber threats. As a non-profit multilateral organisation, IMPACT acts as the platform that enables all member countries to collectively take a global leadership role in the interest of their national cyber-security.

The initiative was formally launched in May 2008 by the Prime Minister of Malaysia, at the World Cyber Security Summit - the largest ministerial-level gathering ever organised on cyber threats. IMPACT's Global Headquarters and permanent secretariat is located in Cyberjaya, Malaysia.



Governments cannot contain the menace of cyber threats exclusively with domestic measures.

Yet, while governments remain largely responsible for the security of a nation's critical infrastructure, the expertise to counter these threats are dispersed across the globe, and in most cases, found outside government hands in the private sector and academia

IMPACT brings together governments, the private sector and academia to prevent, defend and respond to cyber-threats.

IMPACT's International Advisory Board (IAB) comprises a distinguished list of globally renowned experts from industry and academia that together forms a formidable front to effectively address cyber threats.



### Centre for Training & Skills Development

In collaboration with leading global ICT companies, IMPACT will conduct highly specialised training and seminars for the benefit of member governments. Governments throughout the world will gain invaluable insight from the private sector of the latest trends, potential threats and emerging technologies on issues pertaining to cybersecurity.

IMPACT is also a unique platform for member governments to share among themselves some of their 'best practices' and methodologies employed in protecting critical ICT infrastructure, and also in identifying and closing potential vulnerabilities.

Over time, IMPACT will grow to become an invaluable global forum where leading private sector companies can share constructive ideas and solutions with governments of the world. Besides benefiting member governments, participating companies too will gain from the goodwill created and the increased government awareness of their various products and services.



### **Centre for Global Response**

Fashioned after the famous Center for Disease Control & Prevention (CDC) in Atlanta, IMPACT acts as the foremost cyber threat resource centre for the global community complete with an emergency response centre to facilitate swift identification and sharing of available resources to assist member-governments during emergencies.

With a comprehensive database of leading experts from governments, industry and the academia, IMPACT's Global Response Centre is able to act as a 'one-stop' coordination and response centre for countries during emergencies - allowing for swift identification and sharing of available resources across borders.

The Global Response Centre's role also includes establishing a comprehensive Early Warning System for the benefit of all member-countries and providing proactive protection across the globe.



### **Centre for Security Assurance & Research**

IMPACT functions as an independent, internationally-recognised, voluntary certification body for cybersecurity. In consultation with member governments and leading ICT companies, this Centre will help member governments to formulate a checklist of global standards and best practices, creating an internationally accredited benchmark. In addition, the Centre will develop tools such as automated security scorecard systems to further assist governments.

Upon request, IMPACT also has the expertise to conduct voluntary audits on ministries, departments, agencies or critical infrastructure companies (for example: national utility and telecommunication companies) to ensure that those organisations subscribe to the highest international security standards.

In addition, member governments that may find themselves vulnerable to specific or unique threats peculiar to their situation can seek assistance from IMPACT. IMPACT will take on the catalytic role of guiding our partners in academia and industry to embark on research projects to address such issues.

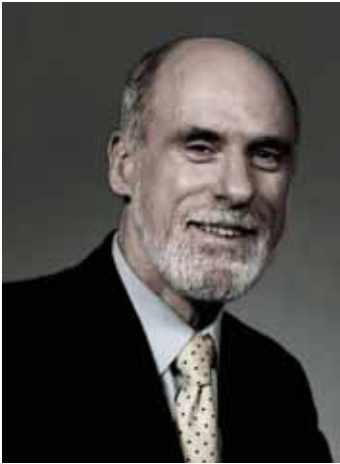


### **Centre for Policy & International Cooperation**

The Centre for Policy & International Cooperation, in collaboration with the ITU and other United Nations agencies, INTERPOL, Council of Europe and OECD, among others, aims to contribute to the development of cyber security-related policies and the harmonisation of national cyber security laws.

Related to this, the Centre conducts and disseminates policy research on current issues related to cyber threats, including cyber crime, cyber law and child online protection. The Centre for Policy & International Cooperation also provides advisory services to interested member countries on policy and regulatory matters relating to cyber security.

Besides this, the Centre aims to create awareness and foster international cooperation through various outreach activities as well as specific programs such as the annual World Cyber Security Summit (WCSS).



**Dr. Vinton Cerf**  
Chief Internet Evangelist of  
Google, 'Father of Internet'

# International Advisory Board

As Vice President and Chief Internet Evangelist for Google, Dr. Vinton G. Cerf is responsible for identifying new enabling technologies and applications on the Internet and other platforms for the company. Widely known as the "Father of the Internet", Dr. Cerf is the co-designer, with Robert Kahn, of TCP/IP protocols and the basic architecture of the Internet. He has been honoured with the U.S. National Medal of Technology (1997) and, together with Kahn, the Presidential Medal of Freedom (2005) which recognised their work on the revolutionary software code used to transmit data across the Internet.

Dr. Cerf's long and illustrious career included playing a key role in leading the development of Internet and Internet-related data packet and security technologies when he served with the U.S. Department of Defence's Advanced Research Projects Agency (DARPA), holding the posts of Vice President of the Corporation for National Research Initiatives (CNRI), Vice President and then Senior Vice President of MCI, and currently Chairman of the Board of the Internet Corporation for Assigned Names and Numbers (ICANN).

He has been a Visiting Scientist at the Jet Propulsion Laboratory since 1998 and has served as Founding President and Board Member of the Internet Society (ISOC). Dr. Cerf is a Fellow of the IEEE, ACM, AAAS, the American Academy of Arts and Sciences, the International Engineering Consortium, the Computer History Museum and the National Academy of Engineering.

Dr. Cerf has received numerous awards and commendations in connection with his work on the Internet, including the Marconi Fellowship, Charles Stark Draper award of the National Academy of Engineering, the Prince of Asturias award for science and technology, the Alexander Graham Bell Award presented by the Alexander Graham Bell Association for the Deaf, the A.M. Turing Award from the Association for Computer Machinery, the Silver Medal of the International Telecommunications Union, and the IEEE Alexander Graham Bell Medal, among many others. He holds a Ph.D. in Computer Science from UCLA and more than a dozen honorary degrees.



## Steve Chang

Founder and Chairman,  
Trend Micro Inc.

Steve Chang is the Founder and Chairman at Trend Micro Inc, a company with over 2,000 employees with sales, operations, research, support and development in over 30 countries. Trend Micro's original focus was to develop antivirus software for PCs, then evolved to addressing antivirus and content security software and services.

Chang also founded AsiaTek, Inc., a Taiwan-based UNIX software design company. He holds a Bachelor of Science in

applied mathematics (Fu-Jen Catholic University, Taiwan) and a master's degree in computer science (Lehigh University, Pennsylvania). His innovative antivirus strategies have earned him recognition: Asia's "25 Movers and Shakers" (ZDNet Asia), a "global force," (Fortune Magazine), twice chosen for Business Week's "Stars of Asia" award which recognised 50 Asian leaders at the forefront of change, and "Innovator of the Year, 2004" (Asia Business Leader Awards).



## Ayman Hariri

Chairman of Oger Systems

Ayman Hariri is Chairman of Oger Systems and a member of the Board of Directors of Saudi Oger Ltd. as well as Chief Executive Officer of Epok, Inc., a US based Company specialising in the advancement of technology for the betterment of global communications. Hariri is also a Board Member of Cell C, a South African mobile telecom operator.

Hariri's successes began within the engineering ranks at the international satellite consortium, Intelsat. Today, he is known for being one of the rare chief executives who combine a deep, hands-on knowledge of complex technology concepts with an impressive history of entrepreneurial success.



## Mikko Hypponen

Chief Research Officer of F-Secure

Mikko Hypponen is Chief Research Officer for F-Secure. He led the team that took down the worldwide network used by the 2003 Sobig.F worm, and stopped several worldwide computer virus epidemics as well. Hypponen was the first to warn the world about the 2004 Sasser outbreak and he named the infamous Storm Worm in 2007. In March 2007, PC World magazine nominated him among the 50 most important people on the web.

Hypponen has assisted law enforcements in USA, Europe and Asia on cyber-crime cases, been a visible IT security spokesperson on major media (CNN, BBC, The Wall Street Journal and Newsweek), written for magazines such as Scientific American, Foreign Policy and Virus Bulletin, and addressed security-related conferences worldwide. He is also an inventor for several patents, including US patent 6,577,920 "Computer virus screening".



## Eugene Kaspersky

Founder and CEO of Kaspersky Lab

Eugene Kaspersky graduated from the Institute of Cryptography, Telecommunications and Computer Science and worked at a multi-disciplinary scientific research institute until 1991. He began studying computer viruses in 1989, when the Cascade virus was detected on his computer. From 1991 to 1997, Kaspersky worked at the KAMI Information Technologies Centre where he developed the AVP antivirus project with a

group of associates (AVP was renamed Kaspersky Anti-Virus in November 2000). Eugene Kaspersky became a co-founder of Kaspersky Lab in 1997.

Today, Kaspersky is one of the world's leading experts in the information security field. He has written a large number of articles and reviews related to computer virology and speaks regularly at specialised seminars and conferences all over the world.



### **Prof. Fred Piper**

Founder of the International Security Group at Royal Holloway, University of London

Prof. Fred Piper is Emeritus Professor of Mathematics at Royal Holloway, University of London and has worked in information security since 1979. He formed Codes & Ciphers Ltd, which offers consultancy advice in all aspects of information security, been consultant to over 80 financial and industrial companies in all five continents, lectured worldwide on information security, published over 100 papers, and jointly authored several books on secure communications.

Prof. Piper has been a member of DTI advisory groups, served on Foresight Crime Prevention Panels and task forces, and

is currently a member of the Scientific Council of the Smith Institute, the Board of Trustees for Bletchley Park and the Board of the Institute of Information Security Professionals, (ISC)2's European Advisory Board, the steering group of the DTI's Cyber Security KTN, ISSA's advisory panel and the BCS's Information Security Forum. Piper has been awarded an IMA Gold Medal for "services to mathematics", and received an honorary CISSP for "leadership in Information Security" as well as an honorary CISM for "globally recognised leadership" and "contribution to the Information Security Profession".



### **Prof. Howard Schmidt**

Former White House Security Advisor; Former Chief Security Officer for Microsoft and Ebay

Prof. Howard A. Schmidt, CISSP, CISM (Hon.), former White House Cyber Security Advisor, is currently the Security Strategist for (ISC)2, the global leader in information security education and certification. He holds a bachelor's degree in business administration (BSBA), a master's degree in organisational management (MAOM) from the University of Phoenix, and an Honorary Doctorate degree in Humane Letters.

A noted speaker and author, Prof. Schmidt has had a distinguished 40-year career in defence, law

enforcement and corporate security. He has also been Vice President, Chief Information Security Officer and Chief Security Strategist for eBay, and Chief Security Officer for Microsoft. He most recently served in the position of Chief Security Strategist for the US CERT Partners Program for the National Cyber Security Division, Department of Homeland Security. Schmidt is also a Professor of Practice at GA Tech, GTISC, Professor of Research at Idaho State University and Adjunct Senior Fellow with Carnegie Mellon's CyLab.



**John W. Thompson**  
Chairman and CEO of  
Symantec Corp

John W. Thompson is Chairman and CEO of Symantec Corporation, and a Board Member of UPS, Seagate and Teach for America, and Chairman of Cyber Security Industry Alliance. Prior to joining Symantec, he had a distinguished career with the IBM Corporation where he held senior executive positions in sales, marketing and software development. In his last assignment, he was General Manager of IBM Americas and a member of the company's Worldwide Management Council.

In 2002, President George W. Bush appointed Thompson to the National Infrastructure Advisory Committee (NIAC), to make recommendations regarding the security of the critical infrastructure of the United States. Thompson has also served as the chair of the Silicon Valley Blue Ribbon Task Force on Aviation Security and Technology. He completed his undergraduate studies at Florida A&M University and holds a master's degree in management science from MIT's Sloan School of Management.



**Dr. Hamadoun Touré**  
Secretary-General of International  
Telecommunication Union (ITU)

Dr Hamadoun Touré is Secretary-General of ITU, has served as Director of BDT, and was Africa's Regional General Manager for ICO Global Communications. Prior to ICO, Dr Touré held several important positions in INTELSAT: Telecommunications Officer, Director for the Africa Region, and Group Director for Africa and the Middle East where he took an active part in the

continental initiative launched by the Regional African Satellite Communications Organization (RASCOM) to pool transponders on the INTELSAT system. He also pioneered studies for regional interconnectivity and worked closely with all African and the Middle East countries to enhance the development of their telecommunication infrastructure.



### **World Cyber Security Summit**

On 20 - 23 May 2008, the inaugural IMPACT World Cyber Security Summit (WCSS) was held in Kuala Lumpur, Malaysia.

The WCSS included the inaugural meeting of the IMPACT International Advisory Board (IAB), a ministerial roundtable, plenary sessions as well as technology and information sharing sessions for in-depth discussion on the latest cybersecurity threats, trends and issues.

WCSS was the largest ministerial-level forum ever organised on cyber-terrorism and security. Government ministers, industry leaders, technology luminaries and international cybersecurity experts from 27 countries were in attendance.

The goal of the Summit was to chart the future course for IMPACT as a global multilateral platform facilitating the partnership between governments, the private sector and academia in combating cyber threats.



### **ITU-IMPACT Collaboration**

At the 2005 World Summit on the Information Society (WSIS) held in Tunisia, world leaders and the UN entrusted the International Telecommunications Union (ITU) with a role to ensure the safety and security of global networks. Recognising that this required a concerted and coordinated international effort by all relevant stakeholders, the ITU responded by launching the Global Cybersecurity Agenda (GCA) as a framework for international cooperation. Bringing together recommendations from over 100 global experts, the GCA spells out key steps that must be taken by the global community for a safer more secure cyberspace.

The close synergies between the work areas of the GCA and the services and infrastructure provided by IMPACT made a joint-partnership a logical step in the global fight against cyber threats, cyber crime and other misuses of ICTs.

In September 2008, a landmark agreement was signed between IMPACT and the ITU, whereby IMPACT was designated as the physical home of the GCA and is now responsible for operationalising the GCA in all of ITU's 191 member states. Under the agreement, all of ITU's member countries also gain automatic membership to IMPACT and are able to access IMPACT's wide range of services, resources and facilities.



# IMPACT

---

INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

[www.impact-alliance.org](http://www.impact-alliance.org)