Green Growth Strategy: a framework for action

Combining economic and environmental objectives is often a juggling act. But 'green' and 'growth' can go hand in hand, and the OECD is working on guidance to help countries and international organisations work towards both these goals

By Angel Gurría, secretary-general, Organisation for Economic Co-operation and Development

"We need clear market signals, such as carbon pricing"

The world economy is slowly, and unevenly, coming out of the worst crisis and recession most people have ever known. While dealing with immediate problems such as unemployment or fiscal deficits, as well as the terrible aftermath of the natural disasters that struck Australia, Japan and New Zealand, the world must look to the future and devise fresh ways of ensuring that the growth and progress that have come to be taken for granted are assured in the years to come.

At the June 2009 meeting of the council of the Organisation for Economic Co-operation and Development (OECD), ministers acknowledged that 'green' and 'growth' can go hand in hand. They asked the OECD to develop a Green Growth Strategy. Since then, the OECD has been working with a wide range of partners, from across government and civil society, to provide a framework for how countries can achieve economic growth and development while at the same time combating climate change and preventing costly environmental degradation and the inefficient use of natural resources. The world needs green growth because risks to development are increasing as economic expansion continues to erode natural capital – which may undermine future growth prospects everywhere for at least two reasons.

First, it is becoming more costly to substitute physical capital for natural capital. For instance, as fish become rarer, more sophisticated boats are needed to catch them. Second, change does not necessarily follow a smooth, foreseeable trajectory. To stay with the fishing example, some fish stocks suddenly disappeared after declining only slowly for years. So to make sure that the progress in living standards of the past 50 years does not grind to a halt, new ways of producing and consuming things must be found. Even what is meant by progress and how to measure it need to be redefined.

This does not mean starting from scratch. Changing current patterns of growth, consumer habits, technology and infrastructure is a long-term project, and the world will have to live with the consequences of past decisions for some time. This 'path dependency' may continue to exacerbate systemic environmental risks even after basic issues, such as incentives to adopt new behaviour, have been addressed. There must also be awareness of possible path dependency in green growth strategies too. Those strategies should be flexible enough to take advantage of new technologies and unexpected opportunities, and to be abandoned if something better becomes available.

The modern economy was created thanks to innovation, and thrives on it. In turn, the economy encourages new ways of doing things and the invention of new products. That will continue to be the case, even though it is notoriously difficult to foresee what form innovation will take. History is littered with examples of intelligent people who got it wrong, such as the *Washington Post* editorialist who declared in 1901 that: "We have … every product of science and accessory of luxury. It seems impossible to imagine any improvement on what we have."

What is known is that without innovation, it will be difficult and costly to address major environmental issues. For example, if two carbon-free backstop technologies in the electricity and non-electricity sectors could be brought to market, then mitigation costs in 2050 would be halved compared with a scenario without such technologies – from about four per cent of global gross domestic product to less than two per cent. Indeed, green technology development is accelerating in some areas. Between 1999 and 2008, the increase in patented inventions in renewable energy (+24 per cent) electric and hybrid vehicles (+20 per cent), and energy efficiency in building and lighting (+11 per cent) was more rapid than total patents (+6 per cent).

While some data are available on green technologies, much less information is available on the related non-technological changes and innovation that will also be instrumental in driving green growth, such as new business models, work patterns, city planning or transportation arrangements. There is some evidence that the scope of green innovation is broadening, however. For example, manufacturing firms have moved from end-of-pipe solutions to approaches that minimise material and energy flows, by changing products and production methods and reusing waste as a new resource for production.

Unfortunately, green and environmental innovation faces additional barriers that exacerbate existing ones. When firms and households do not have to pay for environmental services or the costs of pollution, the demand for green innovation is constrained and there are fewer incentives for companies to invest. Boosting green innovation therefore requires clear and stable market signals, such as carbon pricing or other market instruments, to address environmental externalities.

Governments can support green innovation in three main ways. One is in funding relevant research, whether public or private. Another way is to target barriers to early-stage commercial development, such as access to finance. A third way to strengthen green innovation is to use demand-side innovation policies, for instance standards, regulations or public procurement.

In picking where support should go, there is always a risk of promoting activities that may have occurred anyway. Similarly, there is a risk that more appropriate technologies or practices will emerge that should have been supported, while policy has locked the economy into a less desirable pathway. On the other hand, too little support can prevent achieving policy objectives, so funding approaches need to be tailored to the different stages of technology development. Government funding is most relevant for early-stage technology development, while private finance tends to assume a larger share of later-stage technology deployment and commercialisation.

But no government has all the technological, scientific, financial and other resources needed to implement green growth alone. The challenges are global. This is why green growth is a priority for the French presidency of the G8, whose work "will be coordinated with work done by the OECD". The report to this year's OECD ministerial council meeting is an important step on the road to a Green Growth Strategy. The OECD will continue working with its partners to make a success of the United Nations Conference on Sustainable Development (Rio+20) in Brazil in 2012.

Fishing is an example of a sector in which new ways of producing and consuming things are needed

Recently there have been encouraging international efforts to tackle environmental issues collectively, notably the Cancùn agreements on multilateral action to address climate change. Coordinated international action will also be needed to accelerate the development and diffusion of green technologies, and to reinforce the basic scientific research that underpins them.

Establishing global coalitions to deal with global issues will be difficult, as priorities may differ across countries. Even within a country, the multidimensional nature of green growth strategies will require an unprecedented level of cooperation across government to make sure the policies are coherent. We have set ourselves ambitious targets, but I am confident that by working together we will reach them. ◆

A role for both public and private sectors

With national economic policymakers facing the various challenges of recovery, the G8 needs to be more specific about what governments and the private sector can do to support innovation and generate growth, especially green growth

By Robert Fauver, former US under secretary of state for economic affairs and former G7 sherpa

The 2011 G8 summit takes place during a period of challenge to national economic policymakers. The world economy is now roughly two-and-a-half years on from the global financial market-driven recession. Despite significant macroeconomic policy actions that have been undertaken by the G8 and G20 members, creating a strong, sustained economic recovery has eluded the industrial countries.

In fact, the world is now divided into what the International Monetary Fund (IMF) calls a "two-speed recovery". In the industrial world, recovery has been subdued by historical standards. Unemployment rates have remained stubbornly high, especially long after the recession's trough. On the other hand, the emerging markets have experienced such a buoyant economic recovery that in many emerging markets inflationary pressures have risen and are now complicating policymaking decisions. Monetary tightening in the emerging markets will likely occur this year. This is the first major global recession that has not been eased by the leadership of the economic recovery of the industrial countries. Doubts remain about the ability of the emerging-market economies to lead a sustained global recovery.

After more than two years of stimulus efforts, G8 members face fiscal constraints in their policy choices aimed at supporting domestic economies. Budget deficits – and the associated rising national debt levels – have spooked capital markets in Europe in particular. In the US, the 2010 mid-term elections focused on the historically large fiscal deficits and the sizeable growth in the level of national debt. The now Republican-led House of Representatives has made budget-deficit reduction its first priority for both the current fiscal year and the new budget being negotiated for the fiscal year 2012, which begins on 1 October 2011. The Democrat-controlled Senate has not yet worked out its own deficit position in the form of legislation. Nonetheless, the US budget deficit will be smaller than had been earlier assumed. Keynesian economists bemoan this withdrawal of fiscal support, arguing that domestic economies will weaken without rising deficit spending. However, supply-side and conservative economists believe that reducing the federal deficit will free up resources for the private sector and increase domestic private investment – and facilitating the private sector's ability to fund activities is thought to be the best way to secure a sustainable recovery.

The complicated fiscal problems in some members of the European Union have restrained policy choices significantly and have put pressure on monetary policy choices. Credit-rating agencies have been steadily downgrading the national debt paper of several EU members, essentially down to junk-bond quality. This has led to political efforts to reduce budget deficits dramatically. There is increased concern about the future of the euro, with some arguing that the fixed exchange rate has eliminated one of the major adjustment policy choices for Spain, Greece, Portugal and Ireland. The time-honoured prescription of 'deflate and devalue' is not an

> The emerging markets have experienced such a buoyant recovery that in many, inflationary pressures have risen

option. Some expect that membership in the eurozone will have changed by the end of the year.

Classic macroeconomic policy implementation may have run its course among the G8 members. Most analysts argue that no G8 member has room for new, higher levels of deficit spending. In most countries – with the notable exception of Japan – serious efforts are being made to cut spending, raise tax receipts and reduce budget deficits significantly. This withdrawal of classic stimulus may threaten the expansion path in 2012 and beyond. Monetary policy has been quite loose among the G8 countries, and it too has come close to running its course as a tool for stimulus. Concerns about inflation are being raised, especially in the food and energy sectors.

The March 2011 earthquake in Japan will likely set growth back this year, but the recovery spending and infrastructure rebuilding will improve the outlook for the end of this year and all of next year. Opportunities exist for Japan to undertake policies that target investment in the stricken region and alter its dependence on agriculture.

The G8 must construct mutually consistent fiscal and monetary policies that will reduce governments' borrowing requirements and increase the availability of funds for the private sector. Part of the package should include deregulation and policies that increase the flexibility of various sectors in the domestic economies. In addition, governments must focus on ways to increase productivity and innovation that will provide sustained expansion.

Given the current situation, the French agenda for the Deauville Summit is particularly important. President Nicolas Sarkozy is emphasising two topics new to the summit process that could be important additions to economic policymakers' efforts to secure a lasting economic recovery. Sarkozy has called for discussions of the new challenges for the internet and the role of green growth and innovation in the macroeconomic situation.

Repairing a road after the Japan earthquake. Such recovery spending means the outlook for the country will start to improve

The internet discussions will likely focus on the role of governments in both the development of the global internet and the protection of citizens. This will be the first detailed discussion among leaders of this fast-growing sector of the world economy. They need to focus on whether government actions can strengthen the role of the internet in the global economy. While many would argue that the internet has developed as strongly as it has to date because of a lack of government interference, others would argue that the sector is too important to be left to the vagaries of the private sector. G8 leaders will need to be cautious in their policy interventions in this sector.

Discussions of green growth are becoming a new priority in the wake of the nuclear disaster in Japan. Many had previously concluded that nuclear power must be a part of global solutions to the energy situation and to creating a cleaner environment. But the catastrophe at Fukushima Dai-ichi will likely set back the role of nuclear power for decades. Certainly it will in the US.

Hence, green growth technology will be of increased interest this year. The key to strengthening the role of green growth in the overall macroeconomic picture is to increase productivity through green technology. Worker productivity has been rising only modestly in some members of the G8. In the US, productivity growth has enabled corporations to strengthen balance sheets, but has postponed the rehiring of workers, thus prolonging high levels of unemployment.

The question that has been debated for decades is whether governments can directly support innovation, or whether they can only create a friendly environment for innovation. Direct support may not be as productive as creating a climate for innovation by supporting education, strengthening intellectual protection laws and creating tax incentives for research and development. However, some direct subsidies to support research and regulatory changes to support innovation do work.

Making innovation a commercial success has always been best undertaken by the private sector – at least in the US. Governments have never been creative in commercial markets. For example, new methods of obtaining natural gas from shale have been developed entirely by the private sector. Yet natural gas is one of the cleanest energy sources and contributes significantly to energy production without damaging the natural environment. However, government regulatory frameworks that hinder the development of new energy sources postpone the attainment of both energy independence and a cleaner environment.

The G8 communiqué this year needs to be more specific, and less of a laundry list, than it has been in recent years. ◆

> “Making innovation a commercial success has always been best undertaken by the private sector – at least in the US”

Internet: the way to a bright global future

We can meet the deadline for our developmental and Information Society targets by best utilising communication technologies – in particular, the web. This can only bring social and economic benefits to everyone in the world

By Hamadoun Touré, secretary general, International Telecommunication Union

It is now a little more than half way between the closing of the World Summit on the Information Society (WSIS) in 2005 and the 2015 deadline set to achieve the Millennium Development Goals (MDGs) and the WSIS targets – and it is now abundantly clear that progress towards meeting these can be accelerated only by the smart use of information and communication technologies (ICTs). It is particularly clear that it is necessary to harness the global benefits of a truly global resource: the internet.

The 2011 G8 Summit in Deauville is a good moment to look back at the outcomes of the WSIS process. WSIS was organised by the International Telecommunication Union (ITU), and took place in two phases, in Geneva in 2003 and in Tunis in 2005. It was the most wide-ranging, comprehensive and inclusive debate ever held on the future of the Information Society.

For the first time, governments, the private sector, intergovernmental organisations and civil society all worked hand in hand for the common good. This is a process that continues today with ITU's global mandate to connect the world, working on behalf of all stakeholders to leverage the power of public-private partnerships and bring the social and economic benefits of ICTs to all the world's people.

ITU proactively solicited contributions from stakeholders worldwide throughout the WSIS process. By the time of the Tunis phase there was already significant global consensus on the principles governing ongoing policy deliberations.

At the close of that summit, in November 2005, participants heralded a breakthrough agreement on internet governance that acknowledged the need for enhanced global cooperation. The summit underlined the importance of the development of globally applicable principles for the management of critical internet resources. The WSIS process highlighted the need to address key global issues on a global basis. A good example is accessibility, which is increasingly important in a world where about 10 per cent of the global population, or roughly 650 million people, live with a disability.

To achieve the goal of equitable communication for everyone, ITU, through ITS Standardisation and Development bureaus, focuses on a series of strategic issues ranging from the rights of the disabled to making technical design standards accessible, to providing education and training on accessible ICTs.

Another important example is climate change, which is clearly the biggest issue facing humanity today. In this regard, ICTs are very much part of the solution – because while they are responsible for up to 3 per cent of global greenhouse emissions, they can help to reduce emissions in other sectors by 15 per cent.

> A first step is the development of interoperable standards to protect children online

Close cooperation

ITU works in many areas to use the power of ICTs to address climate change issues. It identifies and protects the necessary radiofrequency spectrum for climate monitoring and disaster prediction, detection and relief. This includes close cooperation with the World Meteorological Organization in the field of remote-sensing applications.

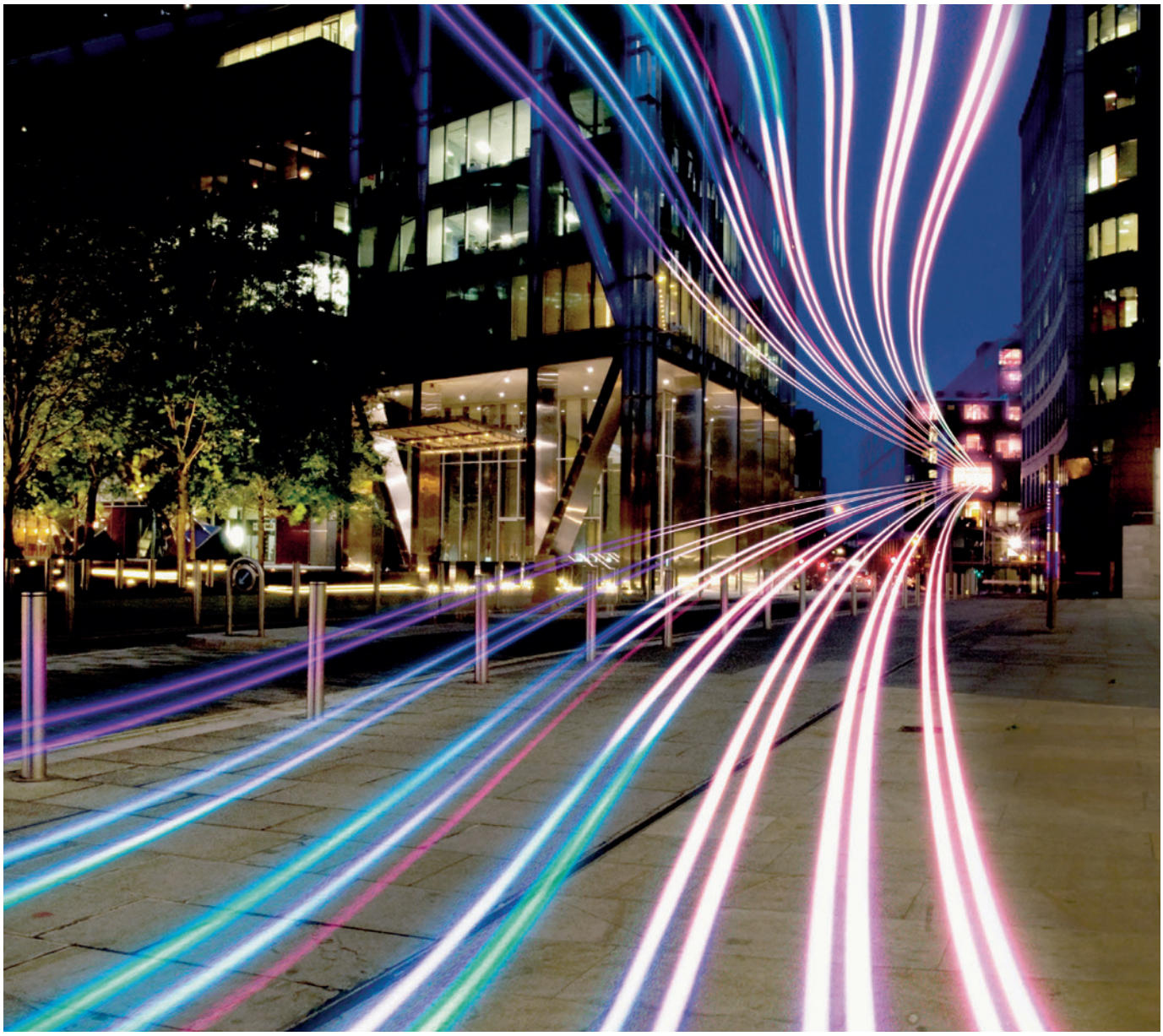
It also develops standards for energy-efficient ICT equipment. It is working on a set of methodologies for assessing the environmental impact of ICT, which includes a global methodology that ICT companies could use to measure their carbon footprint, as well as to estimate the considerable savings in global greenhouse gas emissions and energy that can be achieved in other sectors through the use of ICTs. And ITU continues to help developing countries to mitigate the effects of climate change, including through the use of emergency telecommunications and alert systems for disaster relief.

Cybersecurity was another major area of concern highlighted at WSIS. ITU's concrete response was to launch the Global Cybersecurity Agenda (GCA), an integrated global framework for international cooperation to enhance global public confidence and security in the use of this kind of technology.

ITU is proud to have forged a strong and highly supportive relationship with IMPACT – the International Multilateral Partnership Against Cyber-Threats. As the world's first comprehensive alliance against cyberthreats, IMPACT is the key organisation fulfilling ITU's cybersecurity mandate in an operational sense, providing ITU's 192 member states with access to expertise, facilities and resources to address cyberthreats effectively, as well as assisting United Nations bodies in protecting their ICT infrastructures. More than 100 countries are now part of the ITU-IMPACT operational deployment.

With a globally coordinated approach to cybersecurity, the very real dangers being faced by children and young people online – who often find themselves in cyberspace alone and unprotected – must be recognised. This is why, at the High-Level Segment of ITU Council 2008, the Child Online Protection (COP) initiative was launched, as a multi-stakeholder coalition under the GCA framework.

Since then, ITU has established an international collaborative network for promoting the online protection of children worldwide. Working closely with COP



partners, it created and published four sets of guidelines for policymakers, industry, parents and educators, and children themselves. At the end of last year ITU also published 'Child Online Protection Statistical Framework and Indicators', which is the world's first attempt to provide the overall statistical framework related to the measurement of COP.

With ITU's new patron, President Laura Chinchilla of Costa Rica, the COP initiative is now working to transform its guidelines into concrete activities that will deliver significant national benefits.

Multi-stakeholder approach

The development of interoperable standards and related recommendations to protect children online is a first step. Indeed, standardisation is a key weapon in tackling cybersecurity. ITU international standards facilitated the rise of e-commerce with public key encryption standards; today there is a strong focus on identity management and building an international trust framework for digital identities – a fundamental building block for all cybersecurity, online commerce and child online protection standards.

As the secretary general of the world's oldest intergovernmental organisation, I should emphasise the positive role that can be played by public-private partnerships. By adopting a multi-stakeholder approach, taking into account the needs of government, the private sector, non-governmental organisations, the UN and other international agencies, and civil society, ITU works to build consensus at the global level across all aspects of its work to support social fairness and sustainable development. This multi-stakeholder approach applies as surely to cyberspace as it does to the real world.

International telecommunications regulations need to reflect the changes of the past 24 years

At the end of 2012, at the request of its membership, ITU will hold the World Conference on International Telecommunications (WCIT). The conference will look at ways to revise the current International Telecommunications Regulations, which were adopted in 1988. Those regulations have served the world well, but they need to reflect the significant changes that have taken place over the past 24 years.

In particular this includes the liberalisation and privatisation of much of the telecommunications sector, and also the increasing convergence of technologies and services, which sometimes blur the traditional distinctions between telecommunications and computer technology. Items for discussion at WCIT also include 'security in the use of ICTs', 'numbering misuse', and 'spam', issues that are all increasingly preoccupying the modern world today. ◆

Mobility and security: New economies, new challenges

Since its inception, an important part of the Research In Motion® (RIM) research effort has focused on designing secure and efficient solutions for enterprises and organisations. With its global footprint and millions of BlackBerry® smartphone users, RIM® is particularly well placed to offer its vision to international bodies who are concerned with governance of strategic internet development, the growth of the online world and how the value of secure online communications can be achieved and applied across world markets.

The topic of cyber-security is predominant in discussions of the worldwide growth of mobile data and communications. Cyber-security means securing networks from all attacks, malicious or otherwise. This is best done within organisations through the application of a standard cyber-security policy that both establishes governance of issue resolution and enhances the safety of an organisation, its partners and its customers through the timely and appropriate notification of security vulnerabilities, thereby minimising the risk of exposure and possible exploitation.

The term that signifies the cumulative measures that individuals and organisations take to protect their network assets (personal computers, mobile phones, servers, and so on) is cyber-defence. To understand the impact of cyber-security and cyber-defence in the global conversation, the progress of ecommerce, and the concerns of everyday citizens and governments alike, we must understand the value of security in mobile communications.

A model for internet-driven growth in mobile communications

Communications today have reached unprecedented levels, with information that is readily accessible in electronic forms and that can be easily transferred, duplicated, and shared. Smartphones, portable computers, and tablets are increasingly used by people to access the internet, and particularly in emerging or developing economies, provide the sole connection to the internet.

As the G8 addresses a set of internet-related issues for the first time, aiming to identify new growth and job drivers for mature markets, it serves as an example to other markets that aspire to the same growth. The economic dependency of G8 countries on communication infrastructures will be shared more and more by developing nations. As countries design initiatives to fuel and sustain internet growth in their economies and to protect their consumers, their goals will align with those of G8 countries, including the Europe 2020 strategy.

Globally, people from all walks of life are communicating, buying and selling as part of their daily lives, and the need is stronger than ever for any device or system that transmits data to protect confidentiality in both fixed and mobile environments. Businesses and public-sector organisations alike need to keep their own sensitive data private, but are also responsible for protecting personal information that they store about customers, partners and employees.

The value of security

Individuals and organizations can employ a variety of solutions, including antivirus software, firewalls and encryption, to help protect personal information on desktop platforms. Making these tools available to mobile platform users is a fundamental part of protecting their privacy and earning their trust.

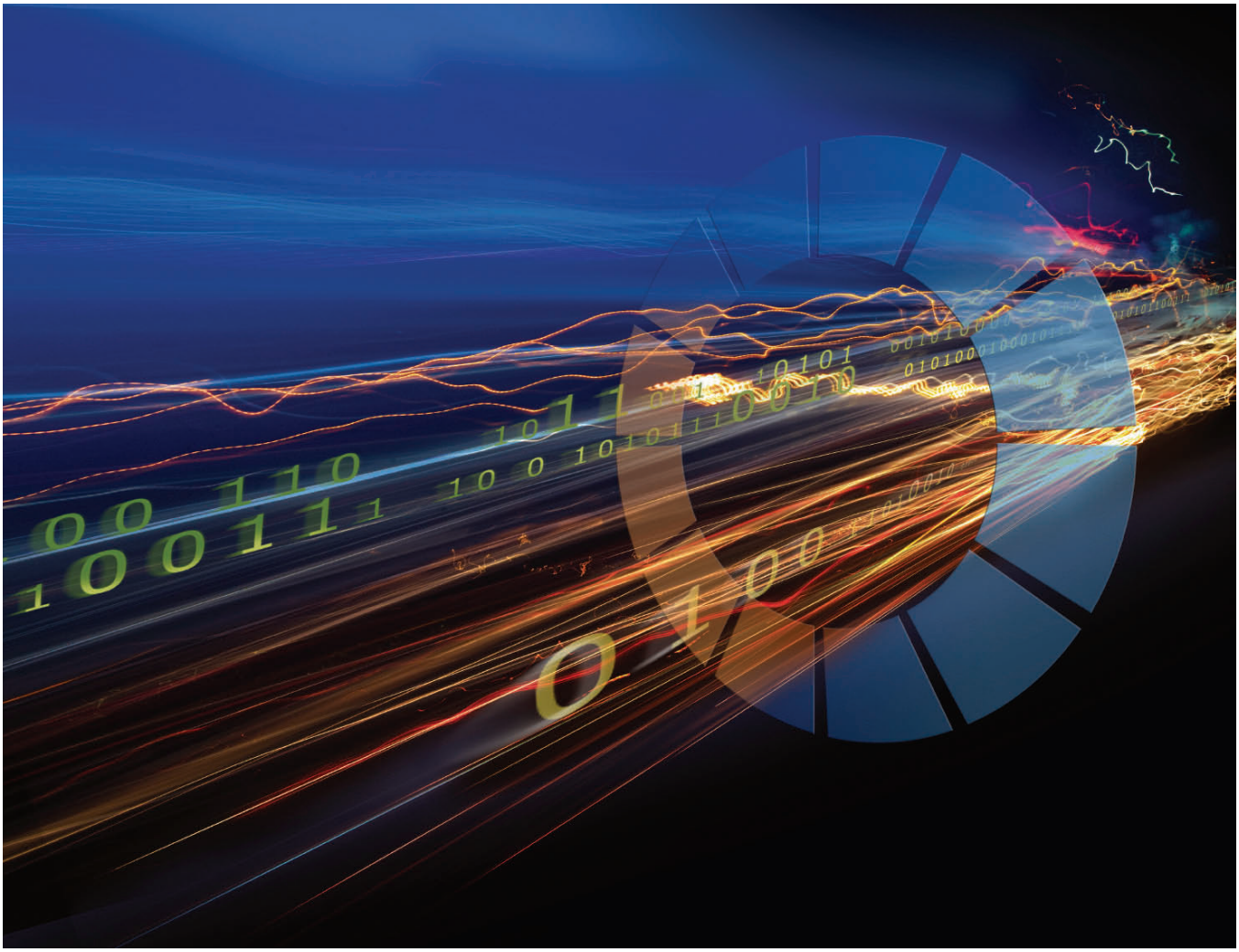
When individuals use mobile devices for personal matters, they still want their personal information to be protected, and they want control over how and when they share it. To meet these demands, communication solutions need to provide built-in security features that allow users to manage their privacy protection easily and consciously.

Security should enhance consumers' choices and be a market differentiator. Consumers must be educated to select solutions that best meet their communications and security needs. Vendors must develop products with security features and technology that appeal to consumers and offer them choice. For example, on BlackBerry® smartphones, a free mobile application for consumers called BlackBerry® Protect allows customers to remotely back up, restore and locate their BlackBerry smartphones from wherever they are via their computer.

Securing the information that users store on their smartphones is a fundamental part of protecting their privacy. The security of a mobile platform should also allow organisations to extend their own data and systems to mobile applications. Mobile business solutions for the public sector must protect information, but allow mobile personnel wireless access to case files and associated records, emergency operating procedures, alert notifications and incident reports – all at the point of need.

RIM firmly believes that security technologies are an important foundation for a digital economy and for the protection of governments and citizens

With up-to-date information right at their fingertips, the appropriate people can receive proactive wireless notification about evolving situations, verify issues with colleagues and take action quickly. Mobile communications technology, provided with the right level of data security, enables a previously unforeseen potential to manage crises and simultaneously protect government and public interests. For example, working with a partner and leveraging their existing BlackBerry® Enterprise Solution, police services in Europe and North America have used custom applications for BlackBerry smartphones that allow officers to access their Records Management Systems. Officers can use mobile devices to make better use of their time on the go and engage with their communities. For more information, see www.blackberrylawenforcement.com/lp/Webinar/LawEnforcementSolutions.html



Conclusion

Whether the mobile device user sending data around the world works for a government organisation, is a business professional or a student, the security of that data matters as much as the mobility of that data. The assurance that sensitive information is secure is an essential cornerstone in developing trust and confidence in the online economy. It is challenging for private citizens to independently verify the security of the mobile technologies they use. To confidently measure and evaluate a mobile solution's security model, many individuals and organisations – including governments and military organisations – look to trusted third parties who have independently verified and certified a technology for use. Security certifications assure people and organisations that the technology they choose is trusted and suitable for use by some of the most security-conscious organisations in the world and may be valuable to the G8, as it looks to assess the risks and challenges of the growth in mobile communications.

About BlackBerry security

RIM has long been a leader in mobile communications and has a history of integrating security features into its products. The company firmly believes that security technologies are an important foundation for a digital economy and for the protection of governments and citizens. BlackBerry products and solutions have received more security accreditations globally than any other wireless solution. The BlackBerry Solution has been approved for level EAL 4+ of the Common Criteria for Information Technology Security Evaluation (CC), the highest level attained by any mobile internet solution designed for civilian use. Security features in the BlackBerry Enterprise Solution include the use of encryption technology, as well as over 500 IT policy controls designed to give organisations the ability to balance individual and enterprise use of BlackBerry smartphones. The BlackBerry operating system has built-in security features to protect stored data and allows individuals to use these same privacy protections for their personal data and the information they choose to allow applications to access. If a device is lost or stolen, encrypted data cannot be read by an unauthorised person. Application controls prevent malware from accessing sensitive personal information.

Over 300 BlackBerry® Alliance Members build out-of-the-box and custom enterprise applications, which people in nearly every industry use on their BlackBerry smartphones to connect directly to and to query databases. For more information, visit us.blackberry.com/business/industry

BlackBerry®

www.blackberry.com/security

Rescuing the global cyber commons: an urgent agenda for the G8

With online demographics rapidly changing, liberal democratic states must lead on new strategic priorities for cyberspace. Security mechanisms should be decentralised and top-down government controls resisted

By Ronald J Deibert, director, the Canada Centre for Global Security Studies and the Citizen Lab, Munk School of Global Affairs

In its short lifespan, the internet has evolved from a laboratory experiment to an entertainment medium, to a global immersive environment – called cyberspace – that encompasses all of society, economics and politics. It is the communications environment in which the world is now embedded. Its constituent parts are widely conceived of as critical national infrastructure.

But alongside its rapid growth and penetration, cyberspace is now entering a period of intense geopolitical contestation as a multitude of actors strive for competitive advantage over and through this new domain. Part of this contestation is driven by a major demographic shift occurring in cyberspace, as the centre of gravity of cyberspace users moves from the North and West to the South and the East. Although cyberspace was born in the United States and other western countries, internet users in China, India, Latin America and Southeast Asia will soon dwarf these early adopting constituencies. The Asian region comprises 42 per cent of the world's internet population – the most by region – but ranks only sixth in terms of penetration rates at 21.4 per cent.

With these new digital natives will come new ways of using cyberspace and different strategic priorities, some of which will invariably clash with the status quo. To understand how cyberspace will look in years to come, one must explore the streets of Shanghai, Nairobi and Tehran. For many of these new digital natives, cyberspace is perceived less as a digital agora than as an opportunity to route around structural economic and political barriers and pursue individual and collective advancement.

The political jurisdictions in which these digital natives reside are entering cyberspace at a difficult historical juncture. For early adopters, cyberspace was governed according to a laissez-faire policy: a domain to be primarily 'left alone'. The states of the developing world – many of them semi-authoritarian or authoritarian – have a much stronger tradition of state intervention in political and economic affairs, and see cyberspace as something to be shaped to preserve collective identity and shore up regime security.

While conventional wisdom has long assumed authoritarian regimes would wither in the face of the internet (and some in the Middle East and North Africa appear to have done just that), many show resilience and capacities that belie the conventional wisdom. Tunisia and Egypt may have succumbed to Facebook-enabled protesters, but China, Vietnam, Iran, Belarus and others have successfully employed control techniques to immobilise opposition, cultivating a climate of fear

and self-censorship. They are also asserting themselves more forcefully in international venues, such as ICANN, the International Telecommunication Union and the Internet Governance Forum, and using regional security forums, such as the Shanghai Cooperation Organisation, to coordinate their policies and seek international legitimation for their territorialised vision of cyberspace.

It may be tempting to portray the contest over cyberspace as a struggle between forces of liberation and control, pitting democratic versus authoritarian regimes. The reality is much more complex. The tradecraft of cyberspace controls comes predominantly from western firms servicing the exploding cyber security market, now estimated to be anywhere between $80 billion and $150 billion annually. Products that provide advanced deep pack inspection, content filtering, social network mining, cell phone tracking and even computer network attack capabilities are being developed by US, Canadian and European firms, and marketed worldwide to regimes seeking to limit democratic participation, isolate and identify opposition, and infiltrate meddlesome adversaries abroad.

Like Eisenhower's military industrial complex before it, this massive cyber-industrial complex is intimately connected to militarisation processes in the West, and in particular in the US. The establishment of US Cyber Command in 2010 helped trigger a major industrial shift in the defence industry and a fundamental force restructuring among allies that is still unfolding.

It also had ripple effects around the world among America's adversaries. These regimes seek comparative advantage by exploiting criminals and patriotic hackers to do their bidding. Major incidents of computer network attacks and espionage have been traced back to the Chinese and Russian criminal underworld. Indian and Iranian officials have gone on public record condoning hackers who work in the state's interest. Not surprisingly, and in the absence of restraints to prevent it, the ecosystem of cyber crime is exploding, providing opportunities for enrichment for the new digital natives and blurring the worlds of crime, espionage and warfare. The world is now witnessing a classic arms race in cyberspace that threatens to subvert the domain entirely.

> In the absence of restraints, cyber crime is exploding, providing opportunities for enrichment for the new digital natives

As the world's largest economies, western liberal democratic countries have a critical strategic interest in sustaining cyberspace as an open and secure commons of information based on freedom of speech and access to information. They also stand to lose the most should it spiral into a hotly contested zone of crime, espionage and warfare. What should be done?

First, a comprehensive strategy to protect the cyber commons should begin by linking the international consequences of domestic policies. If liberal democratic countries pass legislation that permits access to data for state security services without judicial oversight and protections for civil liberties, mandate their armed forces to mount clandestine cyber attacks, use extrajudicial means to disable websites and put internet 'kill switch' powers in the hands of central authorities, there is no moral basis for condemning those actions abroad.

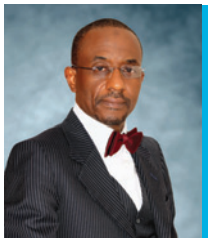
Second, countries should work to build a broad community of like-minded states for supportof 'rules of the road' in the cyber domain. Such rules should include the promotion of norms of mutual restraint, protocols for effective and efficient sharing of law enforcement across borders, and vigorous opposition to the tolerance of cyber crime within territorial jurisdictions. Governments should not be able to hide behind the excuse of attribution challenges when malicious activities originate within their borders.

Third, such domestic responsibilties should include setting standards for the private sector regarding mandatory disclosures of security breaches, strong privacy protections and restrictions on the sale of technologies that assist regimes in the violation of human rights. If self-governance mechanisms such as the Global Network Initiative are insufficient, then regulatory measures should be introduced instead.

Finally, liberal democratic states should lead the promotion of non-state, decentralised and distributed security mechanisms, while actively resisting proposals that alter the constitution of cyberspace through top-down, centralised government controls. Such nascent mechanisms already exist among transnational peer groups of networked computer security professionals and engineers, as well as among academic-based monitoring and research projects. But they need nurturing, financial support and civic empowerment. Federated and decentralised security mechanisms suit not only the constitutive components of cyberspace that should be preserved, but also the tradition of classic republican security thinking that underpins the liberal democratic project.

No longer will it suffice to approach cyberspace in a laissez-faire manner, assuming that leaving it alone will somehow produce benign outcomes. Cyberspace is a human-made domain, and subject to change and manipulation. Liberal democratic governments need a common domestic and foreign policy strategy that creates structural conditions to protect and preserve cyberspace as a secure, decentralised and open commons. Otherwise, future historians will look back at the period of the late 20th and early 21st century as a brief window when such a commons materialised, but then withered in the face of militarisation and short-sighted policies. ◆

Central Bank of Nigeria banking sector reforms



Mallam Sanusi Lamido Sanusi, Governor of the Central Bank of Nigeria

The financial crisis triggered by the sub-prime mortgage crisis in the United States of America between 2007 and 2009, has had a resounding impact on the global economy, Nigeria being no exception. The aftershocks hit Nigeria's financial landscape and the banking system tottered almost to the point of collapse due to the following observable lapses:

- Poor corporate governance practices;
- Overt and undue exposure to the capital market, oil and gas sectors;
- Poor risk-management practices;
- Distress signs through the banks' frequent resort to the interbank market and the Expanded Discount Window (EDW) at the CBN for financial accommodation;
- Inadequate disclosure and transparency about the banks' financial positions.

These developments informed the decision of the new CBN management, led by Mallam Sanusi Lamido Sanusi on his assumption of office in June 2009, to take concrete and pragmatic steps to address the problems.

Policy response

First, the CBN commenced a special joint examination in conjunction with the NDIC to ascertain the true state of the banking industry. The outcome of the examination revealed that a total of eight banks exhibited imminent signs of collapse, which could drag the entire banking sector down, thereby endangering the Nigerian economy.

To stem further deterioration in the condition of the affected banks and protect the interest of depositors and creditors, on 14 August 2009 the CBN intervened with the following measures:

The CBN replaced the executive management and, in some cases, boards of the banks with new ones and referred the cases of some of the principal officers to the law-enforcement and prosecution authorities. One former CEO was recently convicted and other cases are already being tried.

The CBN injected a total of about N620 billion into the banks in form of Tier 2 capital to be repaid from the proceeds of recapitalisation in the near future.

The CBN interventions, as revealed by Governor Sanusi in 2010, were predicated on a four-pillar policy framework:

a. Enhancing the quality of banks;
b. Establishing financial stability;
c. Enabling a healthy financial sector evolution; and
d. Ensuring the financial sector contributes to the real economy.

Besides these measures, the Bank also rolled out other strategies to mitigate insiders' abuse and instil discipline for proactive and risk-oriented supervision, through a new code of corporate governance for the banks and the implementation of risk-based and cross-border supervision in Nigeria.

Other measures include the limiting of the tenure of CEOs of banks to a maximum of 10 years, know-your-customer directives and the comprehensive review of 'fit and proper persons' as managers, directors and major shareholders of banks. All these have helped to minimise the overbearing influence of the CEOs.

In order to boost liquidity and enhance the safety and soundness of banks, the CBN in conjunction with the Federal Ministry of Finance also established the Asset Management Corporation of Nigeria (AMCON), which recently acquired N1 trillion risk assets of some banks. A new banking model was also introduced, which led to the reversal of the Universal Banking Policy, thereby minimising risk and undue adventurism among operators in the Nigerian banking system.

CBN initiatives to revamp the real sector

The CBN Governor, acting in his role as the adviser to the President on economic matters, ensures that there exists some measurable relationship between the real economy and the financial sector. As a result the Bank, in its determination to ensure that there is no disconnect between the banks and the economy, adopted a hybrid monetary policy – a combination of market-based monetary policy measures and direct intervention fiscal-like measures in some critical sectors of the economy. Pursuant to the above objective, the Bank, in collaboration with other stakeholders, took concrete steps, among other actions, to:

- Improve banks' lending to the real sector;
- Empower small-scale entrepreneurs;
- Create employment opportunities;
- Alleviate poverty;
- Ensure food security; and
- Promote youth entrepreneurship

In order to achieve these aims, the CBN initiated a number of schemes and programmes, which included the following:

Infrastructure Intervention Fund (Power & Aviation Intervention Fund)

At its 213th Monetary Policy Committee (MPC) meeting on 1-2 March 2010, the Central Bank of Nigeria approved the provision of N500 billion Infrastructure Intervention Fund as part of the Bank's quantitative measures to create liquidity and support the development of the real sector of the Nigerian economy. Out of the N500 billion, the sum of N300 billion is being applied to power and aviation financing, while the sum of N200 billion was to be utilised for the Refinancing and Restructuring Facility (RRF) of banks' loans portfolio to manufacturing entities. The Fund is financed through a debenture instrument issued by the Bank of Industry (BOI) and subscribed to 100 per cent by the CBN.

Commercial Agriculture Credit Guarantee Scheme

The scheme was established by the CBN in collaboration with the Federal Ministry of Agriculture and Water Resources in 2009 for promoting commercial agricultural enterprises. It is being funded through the issuance of FGN bond worth N200 billion, by the Debt Management Office (DMO) in two tranches.

Under the Commercial Agriculture Credit Guarantee Scheme (CACGS), the sum of N101.38 billion has been released to finance 109 projects made up of privately-owned projects/promoters, and 19 state governments received N1 billion each for disbursement to farmers' cooperatives and unions within their constituencies.

Small and Medium Scale Enterprises Guarantee Scheme

The CBN in 2010 also established N200 billion Small and Medium Scale Enterprises Guarantee Scheme with the aim of promoting access to credit by SMEs in Nigeria. This intervention fund of N200 billion is being managed by the Bank of Industry (BOI), for the purpose of fast-tracking the development of the manufacturing sector of the Nigerian economy by improving access to credit to manufacturers, among other objectives.

Nigerian Incentive-Based Risk Sharing Agricultural Lending

Following the partnership deal between the CBN, United Nations International Development Organisation (UNIDO) and the Alliance for a Green Revolution in Africa (AGRA), the CBN introduced the Nigerian Incentive-Based Risk Sharing System for Agricultural Lending (NIRSAL) in 2010. It is an innovative financing mechanism developed to unlock access to bank financing for agriculture especially through the adoption of risk-sharing approaches to financing. The following have been achieved under the scheme:

- Started securing the buy-in of key stakeholders within Nigerian agricultural financing landscape;
- Consultants have identified eight priority commodities, concluded their financial value chain analysis and those of livestock and aquaculture in progress;
- 15 state governments have subscribed to and accessed N1 billion under the scheme
- Steering committee comprising the CBN Governor, Minister of Agriculture, Finance and Commerce & Industries to give policy directives.

Enterprise Development Centres

The scheme was initiated and funded by the CBN, but is private sector-driven. It is to be established in each of the six geo-political zones of the country, with three already existing in Kano, Onitsha and Lagos. The purpose of the initiative is to, among other aims, develop entrepreneurship among Nigerians and develop skills of would-be entrepreneurs to successfully start up and run business enterprises, as well as link them with financial institutions for start-up capital, especially the microfinance banks.

Committee of Governors' & Bankers' Committee Initiative on Infrastructures

The CBN, under the auspices of the Bankers' Committee, mobilised the commercial banks to finance basic infrastructure projects that will diversify the economy, increase the investment absorptive capacity of priority sectors, and support measures that promote sustainable economic growth. In this regard, for the first time in the Bank's history, in December 2009 in Enugu the CBN held a retreat involving the CBN Committee of Governors and the CEOs of all the 24 banks to map out strategies for growing credit to the real sector. Key sectors such as power, transport infrastructure and agriculture were identified as growth drivers. The banks agreed to meet with willing state governors in order to fund bankable projects they (governors) are sponsoring. Substantial progress has been made in this regard and state governments are taking advantage of this initiative.

Impact of the initiatives

The CBN initiatives undoubtedly served as a catalyst for actualising the vision of the government of Nigeria in bridging the infrastructural gap. It is in this regard that modest progress has been made over the past six months, and it is envisaged that much impact would be attained by the end of the year 2011. Impacts of the initiatives so far are:

- The macroeconomic environment has improved considerably, with inflation moderating to a low double-digit rate;
- The operations of AMCON have started to strengthen the balance sheet of the deposit money banks;
- A remarkable reduction in the cost of funds to the beneficiaries and enhanced credit to boost real-sector activities, leading to multiplier effects on the economy, which has since created thousands of jobs, particularly in the manufacturing sector;
- Significant improvement in the capacity utilisation of companies from 25 per cent to 28 per cent with the reopening of manufacturing companies previously closed for years;
- Remarkable improvements in corporate governance and a better risk-management profile, engendering a healthy and stable financial system, leading to the restoration of confidence in the banking system;
- Increased financing of agric value chain in Nigeria from less than one per cent to two per cent of the banks' loans portfolio;
- Stabilising of operations in the aviation industry, which saved thousands of jobs and enhanced safety;
- Sustenance of Nigeria's global financial and economic rating of BB- by Fitch.

The results so far have been quite encouraging. The CBN shall remain focused and committed to the goal of bequeathing a stable financial system that will oil the wheels of economic development on a sustainable basis.
