Cyber Readiness Index 1.0

Melissa E. Hathaway

Hathaway Global Strategies LLC

No Country is Cyber Ready

by Melissa E. Hathaway

Introduction

In the global economy, national economic growth is largely dependent on information communication technology (ICT). At the same time, many nations are facing significant economic losses due to ICT that undercut that growth. Until now, there was no methodology to evaluate any country's maturity and commitment to securing the cyber infrastructure and services upon which their digital future and growth depend.

The Cyber Readiness Index (CRI), version 1.0, represents a new way of examining this problem, and is designed to spark international discussion and inspire global interest in addressing the economic erosion from cyber insecurity that is holding back more robust economic growth. The CRI examines thirty-five countries that have embraced ICT and the Internet and then applies an objective methodology to evaluate each country's maturity and commitment to cyber security across five essential elements. This holistic approach to evaluating progress towards cyber security demonstrates the importance of a cohesive strategy that includes government regulation and enforcement, as well as market-based incentives and economic levers to focus public and private sector attention on a secure and prosperous digital future.

Background

Over the last fifty years, and in particular the last twenty-five, ICT and the Internet have been at the forefront of technological transformation of critical infrastructures and services, businesses, and society. Today, countries are provisioning near ubiquitous communications to every household and business, and pursuing a development and modernization agenda to nurture their information society into the digital age. Initiatives like e-government, e-banking, e-health, e- learning, next generation power grids, air traffic control, and other essential services are at the top of most countries' economic agenda. These initiatives are being pursued to increase productivity and efficiency, enhance work force skills, drive innovation, and deliver GDP growth. Some estimates offer that when ten percent of the population is connected to the Internet, the GDP should grow by one to two percent.[1] Moreover, governments and businesses that embrace the Internet and ICTs recognize it will enhance their long-term competitiveness and societal wellbeing, and potentially contribute up to eight percent of gross domestic product (GDP).[2] Recent reports go even further and suggest that the opportunity surrounding the modernization of industrial systems (e.g., electrical power grids, oil and gas pipelines, factory operations, etc.) represents a 46 percent share of the global economy over the next ten years.[3]

Nations cannot afford to ignore this economic opportunity, particularly in today's stagnant economic climate. Yet, the availability, integrity, and resilience of this core infrastructure is in harm's way as GDP growth is being eroded by a wide range of nefarious cyber activities. For example, it is estimated that the Group of Twenty (G20) economies have lost 2.5 million jobs to counterfeiting and piracy, and that governments and consumers lose US$125 billion annually, including losses in tax revenue.[4] The United States estimates the annual impact of international IP theft to the American economy at $300 billion. This

approximates to one percent of its GDP.[5] Furthermore, research by Toegepast Natuurwetenschappelijk Onderzoek (TNO), an independent research organization in the Netherlands, has shown that cyber crime costs Dutch society at least 10 billion euros per annum, or 1.5 to two percent of their GDP. This loss is almost equal to the Netherlands' economic growth in 2010.[6] There are other estimates conducted by the United Kingdom and Germany that indicate similar losses. No nation can afford to lose even one percent of its GDP to illicit cyber activities.

Measuring the declining gains may force governments to align their digital agenda and economic vision with their cyber security strategy and invest in the derivative value of both. Bringing transparency to the economic losses may spark national and global interest in addressing the economic erosion. Cyber security initiatives, therefore, can enable and preserve the promise of the ICT dividend and help countries realize the *full* potential of the Internet economy.

The CRI Methodology

The CRI identifies five essential elements where cyber security can be used to protect the value and integrity of previous ICT investments and enable the Internet economy. The initial objective assessment of where each country stands in its maturity and commitment to cyber security can be measured by what steps the country has taken to date on each of these five essential elements. To drill deeper within each of the five essential elements, future studies might add sub-indices to explore in further detail the level of each country's commitment to cyber security.

The five essential elements are:

- Articulation and publication of a National Cyber Security Strategy
- Does the country have an operational Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT)?
- Has the country demonstrated commitment to protect against cyber crime?
- Does the country have an information sharing mechanism?
- Is the country investing in cyber security basic and applied research and funding cyber security initiatives broadly?

First, has the country articulated (and published) a National Cyber Security Strategy that describes the threats to the country and outlines the necessary steps, programs, and initiatives that must be undertaken to address the threat? Ideally, it would: state the strategic problem in economic terms; identify the competent authority[7] - the responsible and accountable entity - that ensures the strategy's execution; include specific, measurable, attainable, result-based, and time- based objectives in an implement plan; and it would recognize the need to commit limited resources (e.g., political will, money, time, and people) in a competitive environment to achieve the necessary economic outcomes.

To explore this area in greater detail, a sub-index might address the following questions:

- What is the gross percentage of GDP embraced by the plan?
- Have commercial-sector entities affected by and responsible for implementation of the plan been identified?
- Have critical services (not critical infrastructures) been identified?
- Have continuity of service agreements (24 hours/7 days a week) and outage reporting

requirements been established for each critical service?

Second, does the country have an operational Computer Emergency Response Team (CERT) or Computer Security Incident Response Teams (CSIRTs)[8] to facilitate national incident response in the event of natural disasters or man-made disasters that affect critical services and information infrastructures?

To explore this area in greater detail, a sub-index might address the following questions:

- Is there a published incident response plan for emergencies and crises? Does it map cross-sector dependencies and address continuity of operations and disaster recovery mechanisms? Is it exercised and updated?
- Are there robust incident management, resiliency, and recovery capabilities for critical services and information infrastructures?
- Has a network of national contact points for governmental and regulatory bodies been established?
- Has a network of national contact points for critical industries that are essential for the operation and recovery critical services and information infrastructures been established?
- Has an information sharing and alert system been established? If so, do the national crisis/response centers address and transmit the alert in a timely manner?

Third, has the country demonstrated international commitment to protect society against cyber crime? For the purposes of the CRI's initial rating, two international treaty agreements were used. The first is the Council of Europe, Convention on Cyber crime.[9] The second is the Shanghai Cooperation Organization, Agreement on Cooperation in the Field of Ensuring International Information Security.[10] The CRI only credits countries that have ratified or acceded to these treaties because only then does a country have a specific obligation and right under international law to uphold its political commitment. Pursuant to these treaties, countries agreed to adopt appropriate legislation, foster international co-operation, and combat criminal offenses, by facilitating their detection, investigation, and prosecution at both the domestic and international levels.

To explore this area in greater detail, a sub-index might address the following questions:

- Is there an accounting mechanism to determine what percentage of GDP is affected by cyber crime (actual loss in real dollars)?
- Is an annual threat assessment to government and critical infrastructure networks prepared?
- Is the country establishing criminal offenses under its domestic law for actions directed against the confidentiality, integrity, and availability of computer systems, networks, and computer data as well as the misuse of such systems, networks, and data?
- Has the country reviewed existing laws and regulatory governance mechanisms; identified where the gaps-and overlapping authorities reside; clarified and prioritized what areas must be addressed first (e.g. existing law (old telecommunications law) and new requirements in the Internet age)?
- Is the infringement of copyright a criminal offense?
- What is the country's ability to fight cyber crime – including training for law enforcement, forensic specialists, jurists,

and legislators – and how has the country's law enforcement system utilized those tools to combat cyber crime?
- Has the country been effective in reducing infections emanating from within its own infrastructure?

Fourth, does the country have an information sharing mechanism that enables the exchange of actionable intelligence/information between government and industry?

To explore this area in greater detail, a sub-index might address the following questions:
- Do mechanisms exist (reporting schema, technology, etc) for cross-sector incident-information sharing, both operational (near-real-time) and forensic (post-facto)?
- Does the government or industry have a rapid assistance mechanism?
- Does the government have the ability to declassify (write-for-release) intelligence information and share it with rest of government and critical industries?
- Is there a government clearinghouse or broker of authoritative information to critical industries?
- Do effective cross-sector and cross-stakeholder coordination mechanisms exist to address critical interdependencies, including incident situational awareness and cross- sector and cross-stakeholder incident management?

Fifth, is the country investing in cyber security basic and applied research (innovation) and funding cyber security initiatives broadly?

To explore this area in greater detail, a sub-index might address the following questions:
- What is the percentage of GDP (or government budget) dedicated to cyber security
  research and development?
- How much funding is dedicated to national research at universities for basic and applied research?
- What is the research/production conversion rate (e.g., percent implemented operationally within the government)?
- What is the commercial adoption of counterpart/ complementary/ subsequent research (or government/commercial) successfully transitioned programs?
- How many universities offer a degree program in cyber security, information security or similar program?
- Is there a government incentive mechanism (e.g., R&D tax credit) to encourage cyber security innovation?
- Is there commitment to interoperable and secure technical standards, determined by internationally recognized standards bodies?
- Is there commitment to protect intellectual property, including commercial trade secrets, from theft?

Selection Criteria

The CRI selected the top twenty countries from the International Telecommunications Union's (ITU) ICT Development Index[11] and the World Economic Forum's (WEF) Network Readiness Index[12] to establish which countries are embracing ICT and investing in accessible and affordable Internet services to promote economic growth. The selection was further refined by adding members of the G20 economies because together they represent: ninety percent of global GDP, eighty percent of international trade, sixty-four percent of the world's population, and eighty-four percent of all fossil fuel emissions. It also brought the largest growing economies of Brazil, Russia, India, China, and South Africa into the Index. Finally, the World Bank's

database and ranking of countries by GDP was consulted. The top twenty GDP contributors added one additional country to the Index. Table 1 lists the thirty-five countries that are included in the CRI.

Table 1: Countries Examined within the Cyber Readiness Index		
The Cyber Readiness Index (CRI) examines thirty-five countries that have embraced ICT and the Internet and compares their maturity and commitment to protecting those investments using an initial objective assessment of where each country stands in cyber security across five areas.		
Argentina	India	Saudi Arabia
Australia	Indonesia	Singapore
Austria	Israel	South Africa
Brazil	Italy	South Korea
Canada	Japan	Spain
China	Luxembourg	Switzerland
Denmark	Macau	Sweden
Finland	Mexico	Taiwan
France	The Netherlands	Turkey
Germany	New Zealand	United Kingdom
Hong Kong	Norway	United States of America
Iceland	Russia	

Initial Findings

The initial findings from the first application of the CRI show that:

- G-20 countries expect at least four percent GDP growth based on the direct and ubiquitous access to communications and ICT adoption rate.
- Some countries lead the index with action in all categories (e.g., Australia, Canada, The Netherlands, United Kingdom, United States), yet even those countries are experiencing GDP degradation due to cyber insecurity.
- 27 of 35 countries have a Cyber Security Strategy, yet few are measuring progress and even fewer have invested in the strategy's successful outcome.
- Almost all countries have an incident response capability either thru a national CERT or through the forum of incident responders.
- 20 of 35 countries are committed by treaty to protect society from cyber crime by adopting appropriate legislation, fostering international co-operation, and combating criminal offenses, by facilitating their detection, investigation, and prosecution at both the domestic and international levels.
- Few countries are investing in private-public information sharing exchanges and even fewer have aligned national R&D initiatives.

Conclusion

Countries are embracing the economic and social potential of the *Internet of Everything* (IoE)— the intelligent connection of people, processes, data, and things. The ITU and the WEF are measuring the benefits that ICT brings to the economy and society. Equally important is bringing transparency to the GDP erosion from illicit and illegal activities that is tearing at the very fabric of our countries (threatening national security and our economic prosperity). Adopting a security framework and knowing cyber readiness level is essential to realizing *full* potential of the Internet economy and our digital future.

The CRI can serve as a solid foundation to help inform this urgent and on-going requirement. While applied to thirty-five countries in this report, it is universally applicable to all countries. It challenges the conventional thinking about cyber security showing that it must be married to the debate and desire for economic prosperity. The CRI identifies the essential elements of a stronger security posture that can defend against the GDP erosion. Moreover, the CRI should spark international discussion about priorities required to strengthen security and encourage governments to take actions and reduce risks.

This index will be updated periodically assessing countries' progress, and evolving evaluation criteria.

Melissa Hathaway is President of Hathaway Global Strategies LLC and a Senior Advisor at Harvard Kennedy School's Belfer Center. She is also a Distinguished Fellow at the Centre for International Governance Innovation in Canada and is the Chairman of the Council of Experts for the Global Cyber Security Center in Italy. She served in two U.S. presidential administrations, where she spearheaded the Cyberspace Policy Review for President Barack Obama and led the Comprehensive National Cybersecurity Initiative for President George W. Bush. Ms. Hathaway is a frequent keynote speaker on cybersecurity matters, and regularly publishes papers and commentary in this field.

End Notes

[1] World Economic Forum, *ICT for Economic Growth: A Dynamic Ecosystem Driving the Global Recovery*, available at: http://www3.weforum.org/docs/WEF_IT_DynamicEcosystem_Report_2009.pdf (last accessed November 5, 2013).

[2] David Dean et al., *The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy*, Boston Consulting Group, perspective 27 (January 2012).

[3] Peter C. Evans and Marco Annunziata, *Industrial Internet: Pushing the Boundaries of Minds and Machines*, General Electric, 13 (November 26, 2012).

[4] Frontier Economics London, *Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy: A Report Commissioned by Business Action to Counterfeiting and Piracy*, Paris: ICCWBO, 47 (2011).

[5] National Bureau of Asian Research, *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property* (May 2013).

[6] TNO, *Cost of Cyber Crime Largely Met by Business*, available at: http://www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=69&item_id=2012-04-10%2011:37:10.0&Taal=2 (last accessed November 5, 2013).

[7] A competent authority is any person or organization that has the legally delegated or invested authority, capacity or power to perform a designated function.

[8] A nationally recognized center that fosters cooperation and coordination in incident prevention, enables rapid reaction to incidents, and promotes information sharing among members and the community at large.

[9] Council of Europe, *Convention on Cybercrime*, Budapest (November 23, 2001).

[10] Shanghai Cooperation Organization, *Agreement on Cooperation in the Field of Ensuring International Information Security* (based on unofficial translation), Yekaterinburg (June 16, 2009). The members of the Shanghai Cooperation Organization are China, Kazakhstan, Krygystan, Russia, Tajikistan and Uzbekistan.

[11] International Telecommunications Union, *Measuring the Information Society: Report 2013* (measured 152 economies).

[12] Beñat Bilbao-Osorio, Suumitra Dutta and Bruno Lanvin (editors), *The Global Information Technology Report: Growth and Jobs in a Hyperconnected World*, World Economic Forum and INSEAD (2013).

