Article

Prepared by: Caroline Shaffer Westerhof,
California National University for Advanced Studies

World's Tech-Ready Countries 2014: Finland on Top Again; Ireland at 26th

MICHAEL HENNIGAN

Learning Outcomes

After reading this article, you will be able to:

- Explain the reasoning that infrastructure is only half of the battle in creating a networked nation.
- Take note of the countries that have moved into the Tech-Ready list's top 10 since 2013, including Hong Kong and South Korea.
- Discuss the observation that the digital divide is not homogeneous.

Country	2014
Finland	1
Singapore	2
Sweden	3
Netherlands	4
Norway	5
Switzerland	6
United States	7
Hong Kong SAR	8
United Kingdom	9
Rep. of Korea	10

World's Tech-Ready Countries 2014: The latest Global Information Technology Report demonstrates that infrastructure is only half of the battle in creating a networked nation. With 90% of its population online, high levels of technological innovation and the concerted efforts of governments, business and individuals investing in ICT (information and communications technologies), Finland once again tops the ranking of the most network-ready countries in the Global Information Technology Report (GITR) 2014 [pdf] produced by INSEAD, the French business school, the World Economic Forum and Cornell University. Ireland got a 26th rank, up from 27 in 2013.

Finland also has something in common with Singapore (2nd), Sweden (3rd), the Netherlands (4th), Norway (5th) and Switzerland (6th). All of these advanced economies have maintained the same leading positions as 2013. Two more Asian countries have nudged into the top 10, with Hong Kong jumping six places to 8th and South Korea moving from 11th to 10th. The United States has risen slightly (to 7th from 9th) and the United Kingdom has fallen two places to 9th.

The report published on Wednesday, says that little progress is being made in bridging the digital divide between technology savvy nations and others. The stalling of progress is worrisome for emerging and developing nations, which are at risk of missing out on many positive impacts ICT bring, including increased innovation, economic competitiveness and greater social inclusion.

Despite the minor shuffles at the top, the story of the winners and losers in ICT-readiness is also a story of ICT inequality. The digital divide between developed and developing countries is widening as emerging nations, despite large investments in ICT, are failing to reap the same big economic and social benefits from technology as their more developed cousins.

It's Not Just About the Wiring

"Large emerging countries are hitting a glass wall," said **Bruno Lanvin, executive director of INSEAD's European Competitiveness Initiative.** "They are not receiving the

of the changes made in ICT . . . there are obstacles to those benefits, especially in talent and skills."

also see that the digital divide is not homogenous," added. "We have a digital divide in Europe between Europe and Southern and Eastern Europe; we have divide in the Middle East, between Gulf Cooperation (GCC) countries on the one hand and North African on the other; and we have other divides in other parts orld."

Matter of Policy

matter, insists Lanvin. "Indeed policies that have to do with ICT specific measures, but also with environment, climate, and the ability to bring foreign investment ct talent. All this is becoming very clear again from the of this year's report." The case of Mauritius demonis fact. Located in Sub-Saharan Africa, a region at the d of the digital divide, the country has managed to rise aces to 48 to become the highest ranking country in the Countries in even more remote areas of development wn the way by being inventive, by being innovative earing their ICT investment to higher levels of comess, growth and job creation," Lanvin added.

Tigers Roar

Russia, India and China (the BRICs) maintained their in the middle of this year's rankings despite pressure challengers. "A few of the BRIC countries are lagging his is not so much due to what the BRICs are not doing ge their ICT systems, but because other countries are ster than them and moving ahead in the rankings," said lbao-Osorio, senior economist of the Global Competiand Benchmarking Network at the World Economic

rising stars in the networked readiness rankings Indonesia which rose 12 places to 64th place and the es which jumped eight rungs to 78.

success, says Lanvin, can be largely attributed to their ical location in a dynamic region where many neighve already forged a path translating ICT investment ng economic growth and social progress. "There are dynamics at play, by which countries can draw lessons experiences of their neighbours. And it's sometimes sier to infer lessons from your neighbours with similar c, social, cultural environments than from other parts orld," he added.

Can Big Data Close the Divide?

Within the ICT landscape what is being called "big data" represents an unprecedented opportunity. The GITR authors say the data boom is akin to the Texas oil boom of the 20th century, calling big data a new asset class.

The ability of companies and governments to sort and structure vast amounts of financial transactions, social media interactions and patterns of human behavior will be reaping what Cisco Systems believes is a US$19 trillion value opportunity.

ICT Ahead

This will also have implications for policy makers. Those able to respond fastest will be able to help their companies and countries succeed. Policies on a range of ICT matters will count even more in the years ahead, the report's authors suggest. "Issues like data privacy and Internet governance will be actively discussed in the coming months, and will determine to a large extent how the world as a whole will be able to take advantage of the IT revolution, and the globalisation of the Internet," Lanvin said.

The Global Information Technology Report uses public data and surveys including an Executive Opinion Survey of more than 15,000 executives polled by the World Economic Forum that gauges usage, socio-economic impact, political, and regulatory environments and the climate for business and innovation, as well as ICT infrastructure, digital content, ICT affordability, and ICT skills.

Critical Thinking

1. What is most at risk for the global economy due to the digital divide?
2. What gives the geographic-neighbor model its value, and how can it be promoted?
3. Can big data close the digital divide, or will it widen it? Explain.

Create Central

www.mhhe.com/createcentral

Internet References

Business Insider: "Finland Needs To Start Advertising How Great It Is"

http://www.businessinsider.com/heres-how-finlands-marketing-problem-has-turned-into-an-economic-problem-2014-10

Computer Business Review: "Who are the world's most Internet-connected countries?"

http://www.cbronline.com/news/who-are-the-worlds-most-tech-ready-countries-in-2014-4220487

Article

Prepared by: Caroline Shaffer Westerhof,
California National University for Advanced Studies

10 Ways to Make the Internet Safe from Cyber Attacks

PATRICK TUCKER

Learning Outcomes

After reading this article, you will be able to:

- Understand why a policy-driven response to cyber attacks is vital to security.
- Describe the European Union's Right to Be Forgotten initiative.
- Discuss the critical importance of being able to function when forced to operate offline.

A single well-designed cyber weapon could "take down the entire Internet," according to Dan Geer, chief information security officer for In-Q-Tel, the CIA's venture capital company.

Here are his 10 policy proposals for protecting the Internet from cyber attacks:

1. Companies Should Be Mandated To Report Big Hacks

We report big disease outbreaks the moment that they happen and the Centers for Disease Control sends out an advance team to deal with them. Why not mandate that companies must do the same thing when they experience a big hack or breach on the federal level? It's a proposal that goes well beyond the largely toothless White House Cybersecurity Framework released earlier this year. It's a move that companies would likely fight, arguing that most of the hacks they face don't constitute the sort of threat that they need to inform the public about. Geer says large companies or the government should have no expectation of privacy in the wake of major cyber attacks, just as individuals with a highly communicable disease lose any expectation of privacy in the event of an Ebola or other major disease outbreak.

"Wouldn't it make sense to have a regime of mandatory reporting for cyber-security failures?" Geer said. "Should you face criminal charges if you fail to make such a report?" He points out that 46 states require mandatory reporting of some cyber attacks in the form of their cyber-breach laws, but 70 to 80 percent of data breaches are discovered by unrelated third parties. Geer says every security failure "above some threshold we have yet to negotiate" should be reported to the federal government. In broaching this, he drew from a recent paper by former Navy Secretary Richard Danzig titled *Surviving On a Diet of Poisoned Fruit*, in which Danzig argues that software hacks should be treated with the same urgency as airplane near-misses.

2. Net-Neutrality Shouldn't Be Left to the FCC

He recommends not one single proposal, but stresses that what's most important to understand is that the Federal Communications Commission is not the sort of agency that can effectively manage something as important to the future as Internet traffic.

"What I can say is that the varied tastes need to be reflected in constrained choice rather than the idea that . . . some . . . agency can assure happiness if and only if it—rather than corporations or individuals—does the choosing."

3. Companies Should Be Held Liable for Making Hackable Software

It's a measure that, had it been in place 20 years ago, Microsoft would be on the hook for every time some piece of malware crashed a computer and Bill Gates would be nowhere near the richest man in the world list.

"The software houses will yell bloody murder the minute legislation like this is introduced, and any pundit and lobbyist they can afford will spew their dire predictions that 'this law will mean the end of computing as we know it!' To which our considered answer will be: 'Yes, please! That was exactly the idea.'"

iking Back Should Be Legal But There Should haps Be Oversight

back is the ability to attack those that attack you. "I at a fair number of you have, in fact, struck back at cker somewhere or, at least, done targeting research u didn't pull the trigger," Geer said. "I'd trust many identify targets carefully enough to minimize collat-ge, but what we are talking about here is the cyber of the smart bomb. As I implied earlier, cyber smart what the national laboratories of several countries ly working on. In that sense, you do know what is behind the curtain, and you know how hard that tar-ly is because you know how hard attribution—real —really is." He called it "expensive therapy" not st small players.

ware Needs Resilient Fallbacks

e makers should be legally obliged to have fallbacks the event of a major attack of service disruption and acks should be in place prior to deployment of the eer calls this resiliency. The best way to assure resil-uild systems that can be managed from afar, so-called aged systems. If you can't build remote management stem, you should design in an expiration date.

ncy is an area where no one policy can be sufficient, ggested a trio of baby steps: Embedded systems mmortal if they have no remote management inter-ded systems must have a remote management inter-are to be immortal, and swap-over is preferable to hen it comes to data protection."

Government Should Pay Top Dollar to Hackers nd Vulnerabilities

alled vulnerability finding and Geer says the U.S. r the market on it and pay people who find vulner-imes what anyone else could pay them for keeping ility secret. Once the government learns of a new , the next step is to make it public.

ole of Texas brothers could corner the world silver is no doubt that the U.S. government could openly orld vulnerability market. That is, we buy them all e them all public. Simply announce: 'Show us a id, and we'll give you 10 times.'" In a subsequent , Geer elaborated further. "Vulnerabilities that you self for use as a future weapon is a hostile act. So he market. . . . If there are a limited number of naking them no longer weaponizable, have we not o world peace?"

ght To Be Forgotten Should Be Put in Place in ited States

pean Union's Right to Be Forgotten initiative, ates that European citizens have a right to have some information kept off the web (or at least out of Google search results), is "appropriate, advantageous [but] doesn't go far enough," Geer said. The definition of privacy that he lives by is this: "You have privacy if you have the effective capacity to misrepresent yourself."

It's becoming a hugely important issue for individuals, but it's not a small issue for the military either. Intelligence agents, Geer says, are having an ever more difficult time keeping their identities a secret. "Crafting good cover is getting harder and for the same reasons. Misrepresentations are getting harder."

In a sense, we are moving toward a post-spy world, according to the guy that runs the CIA's venture capital arm. And protecting the right to be forgotten is one way around that. But more importantly, "a right to be forgotten is the only check on the tidal wave of observability that a ubiquitous sensor fabric is birthing now—observability that changes the very quality of what 'in public' means."

The Obama administration's issuance of a National Strategy for Trusted Identities in Cyberspace is a "case-in-point; it 'calls for the development of interoperable technology standards and policies—an Identity Ecosystem'—where individuals, organizations, and underlying infrastructure—such as routers and servers—can be authoritatively authenticated."

Anonymity is something we give government witnesses and whistleblowers. He says it should be a right for everyone. Moreover, if the U.S. were to follow the European lead on right to be forgotten, it would help curb the balkanization of the Internet, and decrease foreign suspicion of U.S. tech companies.

8. Internet Voting? No

Geer said very little on the question of whether or not the United States or other countries should allow for voting over the Internet or become more reliant on Internet-connected voting machines. But as soon as he said the words, "Internet voting," the crowd in the ballroom of the Mandalay Hotel erupted in laughter and he quickly moved on to the next subject.

9. Abandoned Software Should Be Treated Like Abandoned Stuff

If any company abandons a software codebase then the same rules that apply to discarded furniture should apply to the software—it becomes public and open-source. That means that there would in effect never be any devices out there using software that was proprietary but that wasn't supported. "Apple computers running 10.5 or less get no updates (comprising a significant fraction of the installed base). Any Microsoft computer running XP gets no updates (likewise comprising a significant fraction of the installed base). The end of security updates follows abandonment. It is certainly ironic that freshly pirated copies of Windows get security updates when older versions bought legitimately do not. . . . Either you support it or you give it to the public."

10. Make Sure There's an Offline Backup

"The more we put on the Internet, the broader and more unmitigable Internet surprises become," Geer said. He called this "dependence," and it's a growing problem.

He cited a recent Bloomberg story pointing out that some of the nation's largest banks were calling on the government to protect them from the threat of cyber attack. The article was titled "*Banks Dreading Computer Hacks Call for Cyber War Council.*"

"The biggest financial firms [are] saying that their dependencies are no longer manageable, and that the state's monopoly on the use of force must be brought to bear. What they are talking about is that they have no way to mitigate the risk of common mode failure."

Bottom line: Everything that is a critical infrastructure component *must* show that it can run without the Internet and the makers have to be able to prove it. Geer is proposing a massive stress test for every bank, utility, or any other company that fulfills a critical public role to see how well they operate when they are thrown offline. We stress tested the banks after the 2008 market crash, he points out. "We need stress tests in our field even more."

In his remarks, Geer acknowledged that cyber attacks would get worse before they get better, that maintaining online anonymity would become ever more difficult and inconvenient, and that in the present political environment, many of the proposals would face enormous, if not insurmountable, resistance. Only the second policy proposal has any real chance of passing. But that could change—if things get worse. "There's the political will to do a stress test but only after a bad event. Let's hope it's not catastrophic," he said.

Critical Thinking

1. Of the 10 policy proposals suggested here, which one may be the most difficult to implement? Why?
2. Does the maintenance of online anonymity justify the multitude of inconveniences that are inevitably required? Why or why not?
3. Will anything short of a catastrophe break through the barriers of political resistance when it comes to legislating serious cyber security?

Create Central

www.mhhe.com/createcentral

Internet References

Daily Mail: "Think you're safe on the internet? Think again: Map reveals millions of cyber attacks happening around the world in real time"

http://www.dailymail.co.uk/sciencetech/article-2670710/Think-youre-safe-internet-Think-Map-reveals-millions-cyber-attacks-happening-world-real-time.html#ixzz3JAA9dHls

Entrepreneur: "How to Protect Your Small Business Against a Cyber Attack"

http://www.entrepreneur.com/article/225468

UTG Solutions: "Network Security—Is Your Company Safe from Cyber Attacks?"

http://www.utgsolutions.com/network-security-is-your-company-safe-from-cyber-attacks/

icle

Prepared by: Caroline Shaffer Westerhof,
California National University for Advanced Studies

Reasons Why Sweatshops Still Persist

EEN ONG

rning Outcomes

eading this article, you will be able to:

erstand the relationship between the growth of the rnet and the prevalance of Third World sweatshops.

cribe what a supply chain is and where ethical issues rge within computers and smart phone supply chains.

several reasons why sweatshops exist.

alk to any conscious consumer about sweatshops, and they are likely to ask you—"what company *is* 'sweat free'?"

answer is not simple. Although some companies do a etter job than others, it's easier to name companies that sweat-free. Strictly talking about factories that produce ort to global retailers, supply chain management prac- n enable sweatshop conditions. Since the term 'sweat- describes abusive workplace conditions, consumers be conscious of how this happens, to ask the right ques- d become part of the solution.

e are 7 key supply chain realities, which can help us see eatshops persist:

ot Just in China

hops are everywhere. Bad working conditions tend espe- be prevalent in workplaces where there are migrant eless' workers, as labor law does not usually protect Additionally, workers who lack basic education have ices for work. For example, forced labor in Florida's fields, and child labor in Malaysia's palm oil indus- often stateless and/or migrant workers. The bargaining f these workers is absent, and their disenfranchised sta- les exploitative practices.

2. Most Brands Don't Own Their Factories

Almost every large retailer is vertically disintegrated. Aside from Foxconn, it is rare for the general public and mainstream media to know the name of a supplier factory. Vertically disintegrated business models decrease the liability for companies if something goes wrong at the factory, and increase their flexibility in buying. But a retailer's responsibility for their transactional relations is still going to be questioned by the public and media, as their brand reputation is inextricably linked to their social responsibility. A customer wouldn't return a defective shoe to XYZ factory where it was produced in Indonesia, they would return it to the Nike store where they bought it. But, would customers return a shoe if they found it was produced by exploited workers?

3. Unstable Relationships Create Risky Circumstances

Companies might have policies for issues such as forced and child labor, as well as an ethical code of conduct, but in the end it all comes down to the purchase order. Often, but not always, the supplier has a comparably smaller voice and decision-making power than its retail customers. Many suppliers are faced with short-term contracts and inadequate lead-time to produce goods. If a factory doesn't have the security of a long-term customer relationship, it may need to front its own money, and therefore will be fighting to make every purchase order happen on time, by any means necessary. This triggers excessive overtime, which can trigger an increase in workplace accidents and defective products, as well as illegal subcontracting as we've seen in the case of Zara. For retailers, it is important to ask: *does the supplier actually have the capacity and time to produce what we're asking for in the ethical manner that we seek?*

4. The Purchase Order Determines the Degree of Influence

Supplier factories are independent businesses, and their customers are retailers that buy their goods. A scarf factory in India can be producing for 80 brands, and as a result, be audited by different retailers' code of conduct auditors 2–3 times a month. Foxconn wasn't just producing for Apple, it was also producing for others such as Sony and Intel. It's important to see where the money flows and how often, to determine the degree of influence exerted to follow the retailer's code of conduct. For retailers, before suppliers are expected to broadly respect human rights, it's important to do a reality check—*what percentage of the supplier's business are you? Do you have a long-term contract with them?*

5. Audits Alone Don't Create Change

Alone, audits of codes of conduct or voluntary standards are seldom able to change workplace conditions, nor provide a guarantee. Auditors take a snapshot of the factory at a given time and place. Supplier factories will do what is *expected* and *inspected*. Ultimately, it is what is done with the information found in the workplace, whether by an auditor or anyone else, that effects change. On May 20, 2011, an explosion caused by a buildup of aluminum dust killed three workers at Foxconn in Chengdu. Just two days earlier, SACOM publicly documented this as a health and safety violation in a report, after witnessing workers enter Foxconn with aluminum dust coated in their skin and hair. No action was taken in time.

6. Ethically-Made Products Are Not Always More Expensive

Price elasticity varies by product, sector, consumer base, and in the case of Apple—cult following. On the eve of the iPhone 5's release, news reports described the crowds of people that waited outside the Apple store. Consumers were selling their spot in line, and previously there was a report that one consumer sold his kidney to buy an iPad and iPhone. If a price premium were definitively established to ensure an ethical product, would consumers purchase it? Of course this depends on the circumstances, but according to a Harvard case study on ethically labeled towels, coffee and shirts, the answer is—yes, they would.

7. Misaligned Incentives and Unintegrated Retail Departments

In the past decade, many companies have established 'Corporate Social Responsibility' (CSR) departments, where some focus on managing human rights in their supply chains. Chances are, these departments are silos. If they are not closely cooperating with the other departments that communicate with suppliers, conflicting messages that produce misaligned incentives may occur. For example, the questions suppliers receive might differ substantially:

- Purchasing Department: "Can you produce this by next week?"
- Design Department: "Can you change this now?"
- CSR Department: "Can you cut overtime to legal limits?"

It is important that all departments are integrated with similar goals, objectives and incentives about the code of conduct at the design stage. Otherwise, the supplier might only listen to the department that issues the purchase order.

These are seven key realities about sweatshops I've encountered in my daily work at Social Accountability International (SAI). Can you think of any others?

Critical Thinking

1. In what ways are the use of Third World sweatshops an Information Technology problem? In what ways did the advent of the Internet exacerbate the problem of sweatshops?
2. Why is it difficult for brands to simply decree that sweatshop labor will not be used to create their products?

Create Central

www.mhhe.com/createcentral

Internet References

Apple Supplier Foxconn Pledges Better Working Conditions, but Will it Deliver?
www.pbs.org/newshour/bb/world/jan-june12/apple_03-30.html

Will Technology End Sweatshops?
www.monroenews.com/news/2013/jun/02/will-technology-end-sweatshops/?news

Workers' Rights 'Flouted' at Apple iPhone Factory in China
www.theguardian.com/technology/2013/sep/05/workers-rights-flouted-apple-iphone-plant

The World's Least Wired Countries, in 1 Map
www.washingtonpost.com/blogs/the-switch/wp/2013/08/21/the-worlds-least-wired-countries-in-1-map