Scenario: Regionalization of the Internet

While most of us have a sense of – and preference for – the "unitary" internet we have today, the web as we know it is already developing into a series of "Internet Islands" or regional divisions based on geographic and/or economic similarity. Natural and man-made disasters could easily accelerate this process, leading to an alternate future where the differences between these islands is more pronounced and e-conflict between regions becomes a significant national security and economic development issue.

Key drivers for this scenario included:

- National and corporate security concerns and increased pressure from non-state actors based in "failed state" regions of the world
- Global economic weakness, budget crises and significant, systemic unemployment
- Shortages of food and raw materials leading to rises in the prices for commodities, food and energy and supply chain/trade disruptions
- A rising "black market" dominated by narco/political/religious groups with increasing technical sophistication
- Expansion of iPV6 and the "internet of things" creates an environment where citizens can be easily tracked within a region and where a market in false identities flourishes

2011

In 2011, Internet governance follows the loose "Reston Consensus" (named for the city where the commercial internet established its first real "roots" in Northern Virginia), with major players in business, the NGO world and academia agreeing to a kind of managed competition based on the concept of a unitary internet. A multi-stakeholder approach to Internet governance appears to be the right model.

Governments push for more control in international forums, but the consensus holds as most people in developed markets argue that it is unnecessary to fix a system that has worked so well, and most internet users in developing regions are still focused primarily on issues around access and narrowing the digital and e-commerce divides.

However, with time a series of man-made and natural disasters put pressure on the fragile, talk-shop-oriented governance models. A combination of government's inability to act in some regions and heavy-handed government action in others, as well as the emergence of creeping vulnerability to both government-sponsored cyber aggression and non-state rogue actors increases the sense of the need for regional alliances for security on the web. Regional islands, once an obstacle to be bridged with sturdy causeways, become increasingly seen as crucial to security – providing protection with regional drawbridges that can be lifted to create safe havens from danger and prevent contagion from outside.

2012-13
By 2013 political liberalization in the Arab world had accentuated divisions within the region, with authoritarian regimes reestablishing control in many states, leveraging the same social media tools that had been used to put them under pressure in 2011. New democracies in the Mediterranean region, unable to address short-term needs for employment, and reduce prices for food and staples, foundered, giving rise to an inward-looking conservative backlash in the form of political movements skeptical of Internet openness and increased calls for regulation on the web.

At the same time, massive droughts in East Africa led to widespread hunger, a further deterioration of the Somali state, and massive corruption, as aid trapped at ports like Mombasa were increasingly siphoned off and re-sold by criminal gangs that had hacked into the port's logistics system. Aid agencies first tried to cover up then admitted the losses, but the damage was done. Regional governments and NGOs seemed powerless to get control over the system. Refugees were on the move all over the region, seeking food and shelter. The region's e-government systems proved inadequate for the task, and the pace of progress toward internet-enabled development slowed, as legislators were called upon to "protect the masses". Web-enabled criminal enterprises see clearly how they can leverage failed states to create short term gain based on chaos.

2013-15
The combination of continued budgetary challenges in the southern parts of the Euro zone, rising energy and food prices puts additional pressure on those countries already struggling with long-term high unemployment. Cash-strapped European governments increasingly see the Internet as a potential source of revenue, and move to push companies to "Buy European" in the e-commerce world, further emphasizing the growing sense of Europe as a "regional island". At the same time, these attempts to create cyber-tariffs and preferences lead to increasing tax evasion and other efforts to beat the system, hurting consumer confidence and increasing the online role of organized crime (the so-called "digital cartels").

2016-20
China's Internet growth explodes, with mobile-web enabled Chinese citizens becoming more than one third of all web users worldwide. To keep control internally, the Communist Party emphasizes iPv6 expansion and creates a model "internet of things" protocol, allowing the government to increase its tracking of citizens' movements and political speech, but also their shopping preferences, creating a huge new source of market data on the world's largest pool of consumers. Externally, the country increasingly flexes its muscles in the Internet governance world, pushing a government-centric "safe home" vision of the internet's future in a newly-government dominated IGF and in the ITU, where likeminded governments create the "safe home bloc". As part of this effort, the country uses its market power to stifle international private sector criticism, since firms who propose an alternate vision of the web risk being frozen out of the Chinese market altogether.

At the same time, massive floods and earthquakes in Central Asia further isolate this region, and climate change makes the production of both wheat and opium nearly impossible. With the US and NATO beset by budget crises, weary of war and desperately trying to disengage from the region, lawlessness rules in many remote areas while unemployment tops 80%. Local warlords move from exporting drugs and radicalism to providing havens for cyber-terrorists who are beyond the reach of any kind of government or law enforcement. From this platform, shady groups develop ever stronger tools to attack, extort and steal from businesses and individuals around the world.

And finally, after nearly a decade of building up the region's mHealth and eHealth infrastructure and moving totally to telemedicine and electronic patient records, the Southern Africa health system collapses. The cause is unclear, and rumors abound that an opposition group or crime syndicate might be responsible, but the region is plunged into chaos.

2025

The world has become increasingly web-dependent – despite the desperate challenges to cyber security and online commerce. The vision of cooperative, global Internet governance is long gone. Regional and political blocs arise, but even within them governments have limited ability to protect citizens from cyber-predators.

Lives have become so stressed that it is routine to perform "network intersessions" where top officials are spirited away for extended periods of time to areas completely off the grid in order to "detox" from the network. Indeed vacation resorts are established that specialize in offering completely isolated areas that block even satellite connectivity as the medical profession attempt to cope with the new "addition" to the network.

China, once considered THE rising global power, is beset by internal conflict as the global economic downturn curtails growth and population continues to grow. Elites with access to the state's large data network can make colossal fortunes, while upward mobility by most Chinese is stopped cold despite greater use of technology.

Population growth, climate change and increasing urbanization globally lead to massive food and resource scarcity, as well as regional competition. Only well-networked elites can move smoothly to take advantage of international trade.

Within your region, on your island, there is no real privacy. Government, in the name of national security, has gained access to your data. But there is the potential of anonymity if you move, since your digital footprints are washed away once you leave your island. For those that can afford them, a black market in digital identities (IPv6 addresses and phony addresses) leads to the ability for anyone or at least everybody with resources, to "buy" multiple identities.

In the end, the promise of a boundary-free world has turned into a the reality of a world dominated by black market instability, where trust – the cornerstone of the early web – is hidden behind ever higher regional walls which restrict trade but don't succeed in really keeping out danger.