FT.com
FINANCIAL TIMES

By Misha Glenny
Published: March 18 2010 02:00 | Last updated: March 18 2010 02:00

It is time to stop thinking of cyberspace as a new medium or an agglomeration of new media. It is a new continent, rich in resources but in parts most perilous. Until 30 years ago, it had lain undiscovered, unmined and uninhabited.

The first settlers were idealists and pioneers who set out from San José, Boston and Seattle before sending back messages about the exciting virgin lands that awaited humanity in the realm of the net. They were quickly followed by chancers and adventurers who were able to make fortunes by devising their own version of the South Sea Bubble.

It was inevitable that the wondrous materials found all over this territory would attract the interest of nation states. Now, the scramble for cyberspace has begun. Military and intelligence agencies are already staking their claim for the web's high ground as civilian powers lay down boundaries to define what belongs to whom and who is allowed to wander where.

Cyberspace is being nationalised rapidly. In some parts of the world, this has been going on for a while. Russia has been running a programme known by the delightfully sinister acronym Sorm-2 (System of operational investigative activities) since the late 1990s. This ensures that a copy of every single data byte that goes into, out of or around the country ends up in a vast storage vault run by the Federal Security Service. You can read about atrocities committed in Chechnya if you wish but you can be confident that somebody will be looking over your digital shoulder.

China, of course, has its "great firewall", filtering politically incorrect sites along with pornography and other forms of cultural contamination. But of even greater import is China's demand, effectively conceded, that the US relinquish control of the internet's language and domain names through the Californian non-profit organisation Icann. This is being transformed into a United Nations-style regulatory operation. China will soon have absolute say over the internet's structure within its borders.

The legal mapping of cyberspace in the west is more chaotic. But we are now witnessing the establishment of myriad laws and rules by legislators and in the courts. In a hearing this week at Blackfriars Crown Court in London following a major cyber-crime trial, Harendra de Silva QC put his finger on it when he argued that "we are entering a world where almost any human interaction of any kind will require use of the internet".

So while there is clearly a pressing need to define rules that apply in cyberspace, they are emerging at speed with little coherent strategy behind them. Nobody knows where this process will lead for two central reasons. The speed of technological change means that the traditional tools of state used to carve up the world in the 19th century, such as laws and treaties, are often inadequate if not entirely irrelevant when applied to this new domain.

Law enforcement agencies such as the FBI and the Serious Organised Crime Agency in Britain have invested considerable time and money in bringing down criminal networks on the web. But as the Internet Crime Complaints Center in the US has just reported, the losses from cyber-crime continue to climb at a staggering rate because criminals adapt at lightning speed to new policing methods.

In the commercial world, major legislation concerning copyright, such as Britain's Digital Economy Bill, is unlikely to withstand the second great variable - the coming of age of the net generation. Laws banning file-sharing are likely to prove as unpopular as the poll tax that helped bring down the Thatcher government. They also look utterly unenforceable.

As a harbinger of change, we are seeing political parties springing up throughout Europe with names such as the Internet party or the Pirate party, which understand the web as simply part of human DNA. "In the collision between the old and the new on the web," argues Rex Hughes, a Chatham House fellow who is leading a cyber-security project, "the old always wins the first few rounds but eventually they die off".

But the greatest battle is happening in the area of cyber-warfare and cyber-espionage. Symbolically, the US designated cyberspace as the "Fifth Domain" last June and the first man-made one after land, sea, air and space. Nato lawyers are trying to work out how the laws of war operate in cyberspace. Hysteria is accompanying this new arms race, as when Admiral Mike McConnell, former director of US National Intelligence, claimed at a Senate hearing last month that "if the nation went to war today in a cyber-war, we would lose".

Meanwhile, the phenomenon of "anonymisation", so useful for cybercrime, is a gift to intelligence agencies as they sniff into every corner of the web to find out who is up to what.

None of this would amount to a hill of beans were it not for Mr de Silva's point that everything we do is somehow mediated by the web. Governments are becoming obsessed about the need to control the internet but have yet to work out how to do this without suffocating the noble goal of those pioneers who merely wanted to facilitate communication between ordinary people. Heaven forbid!

The writer's latest book is McMafia: A Journey through the Global Criminal Underworld