Disagreements on cyber risk East-West ''Cold War''

Peter Apps, Political Risk Correspondent, Reuters

With worries growing over computer hacking, data theft and the risk of digital attacks destroying essential systems, western states and their allies are co-operating closer than ever on cyber security.

But as they do so, the gulf between them and China and Russia - blamed for many recent hacks and with a very different and much more authoritarian view over the future of the Internet - grows ever wider.

Last week, Chinese officials turned down invitations to a privately run conference of military and civilian experts on cyber security in London, telling organizers Defence IQ they would not attend due to a "low tide" in relations with the US, particularly its military. A senior Russian official also pulled out at the last moment, citing a failure to obtain a UK Visa in time - although other attendees suspected that might simply have been an excuse.

Western officials talk down such snubs. But they admit progress towards international agreement on "norms of behavior" in cyberspace remains a distant dream.

"It is worrying," says John Bassett, a former senior official at British signals intelligence agency GCHQ and now senior fellow at London's Royal United Services Institute. "If anything, in the last year the differences have become more apparent and there seems to have been little success in tackling them. There is a risk it could end up damaging the wider relationship."

Russia and China, it seems, have little appetite to tackle data theft whilst the West has no intention of acquiescing to Russian and Chinese demands for a more controlled Internet.

Jim Lewis, a former U.S. foreign service officer and now senior fellow at Washington DC think tank the Centre for Strategic and International Studies, participates in regular semi-official meetings with China on cyber.

"There are several things coming together here," he says.

"There is the political difference over the freedom and future of the Internet. Then that gets tied together with the theft of commercial property - which itself becomes part of the wider trade issues."

Already, Western officials and academics involved in talks say discussions on cyber between East and West have become much more difficult and more complex than on any other issue.

"This is going to be a very gradual process," says Christopher Painter, the US State Department lead official on cyber policy. "There are obviously some very different visions of the future of the Internet ... On intellectual theft, I'm not going to single out China or Russia but it's obviously something we take very seriously."

A November London conference organized by British Foreign Secretary William Hague was supposed to kickstart progress towards global consensus. But if anything, it looks to have simply exacerbated the differences. A follow-up conference in Budapest later this year could be similar, some fear.

"The London conference did seem to show a "non-flexible" attitude from both the West and East," says Tony Dyhouse, a leading cyber security specialist for UK defense firm QinetiQ. "Dare we coin the term 'Cyber Cold War'?"

INTELLECTUAL PROPERTY THEFT

In public, U.S. and other Western officials almost always decline to detail where they believe the plethora of recent cyber attacks have come from.

In the last year, they have included attempts to break into computer systems at the U.S. State Department and British Foreign Office and other highly publicized attacks on Lockheed Martin, Google, the NASDAQ and the International Monetary Fund amongst others.

But privately and occasionally on the record, they frequently point the finger at Russia and China. Both angrily deny any involvement, saying they too are victims of hacking.

But many Western security specialists say the evidence against both nations - particularly China - has become increasingly compelling.

"China is currently engaged in a maximal industrial espionage effort that it justifies internally in terms of a catch up strategy (with the West)," says Thomas Barnett, chief analyst at political risk consultancy Wikistrat and a former strategist for the U.S. Navy. "The key question here is: can China assume the mantle of intellectual property rights respect fast enough to avoid triggering economic warfare of the West... If it can't, then this is likely to get ugly."

PricewaterhouseCoopers consultant Tim Hind, a former intelligence chief at British bank Barclays, has few doubts.

"I think government circles and organizations now ... have very good attribution," he says. "The question is what you do diplomatically with that attribution ... I think our government sees our economic and political mission with China as more important than addressing the cyber issue."

Some believe the most promising avenue of negotiation might be to link it to one of Beijing's primary worries - the buildup of US military forces in Southeast Asia.

"There is a deal to be made here involving the U.S. ceasing its intelligence gathering, naval and air activity off China's coast," Nigel Inkster, a former deputy chief of Britain's Secret Intelligence Service (MI6) and now head of political risk and transnational threats at London's International Institute for Strategic Studies, said late last year.

But others suspect the scale of Chinese responsibility might be overstated.

"One thing is certain - the "in thing" to do is blame China and hence it is likely that at least some of the actions blamed on China will not be of that origin," said another European cyber security expert, speaking on condition of anonymity. "They've become a "no questions asked" scapegoat."

Because of the focus on China, some experts say the scale of hacking from Russian territory is often ignored.

That, some suggest, is how Moscow was able to marshal so many "patriotic hackers" to paralyze Estonia's Internet during a political face-off in 2007 as well as attacking Georgian websites during the 2008 war. More recently, such hackers have targeted dissident websites.

VAST PHILOSOPHICAL GULF

Perhaps even more serious than worries over hacking, however, is the vast philosophical gulf between East and West.

Last year, both Russia and China saw a rise in Internet-fuelled unrest that they blamed in part on the West. Beijing's censors increasingly struggled to control micro-blogging on their relatively tightly regulated Internet, whilst recent protests against Vladimir Putin are seen further fuelling Russian desire for control.

In the run-up to the London meeting, Moscow and Beijing released a suggested "code of conduct" for the global Internet that would give national governments much more control over the Internet within their borders.

But Western states swiftly shot down such suggestions. Despite British hopes the Chinese and Russians would not feel "ambushed" at the London summit, they would have found much to dislike there.

"The Chinese see the Internet as an American construct, designed to provide the U.S. with military and commercial advantage," said Lewis, adding that Beijing suspected the West of fostering dissent within its borders as well as building powerful cyber weaponry with which to attack.

With almost every nation dramatically ramping up its military spending on cyber security - including offensive "cyber warfare" capabilities to attack essential networks, turn off power grids and cause massive disruption - some fear more serious confrontation.

In a worst-case scenario, a single damaging cyber attack could spark a wider conventional war or even nuclear confrontation - with the risk a nation might wrongly blame a rival government for the actions of a single hacker and strike back. The 2009 Stuxnet computer worm attack on Iran's nuclear program that reprogrammed sensitive equipment to tear itself apart was seen by many as a sign of things to come.

As with any potential military conflict, experts have long said the key to avoiding accidental escalation is the creation of "confidence building measures" between all sides such as meetings, hotlines and shared discussions over threats.

Senior officers from the newly launched U.S. Cyber Command and other officials have massively ramped up links with other military and civilian cyber agencies across NATO and the Western world. That process with China and Russia is at a much earlier stage, officials say. Some believe more should be done.

"Even if you have long-running cyber arms control negotiations that never really went anywhere, that would give you the chance to get conversation and contacts going," says former GCHQ official Bassett.

For now, many believe the greatest risk is that paranoia sets in on both sides, further entrenching positions.

"We are very tempted by a "Cold War" way of thinking," says Lewis at the Centre for Strategic and International Studies. "The problem is that that can be very self-fulfilling."

(Additional reporting by William Maclean and Tim Castle)

(This story was corrected in paragraph 13 to change the spelling of UK defense firm to QinetiQ)

Posted by Jason Lomberg, Technical Editor