RSIS COMMENTARY

www.rsis.edu.sg No. 009 – 10 January 2017

Fight in Cyberspace: The State Strikes Back

By Eugene EG Tan

Synopsis

Ensuring that the state is secure from cyber threats is increasingly becoming the priority of states all over the world, sometimes clashing with concerns over privacy. There are four notable ways that states have increased their presence in cyberspace in 2016, and this presence is forecast to become more prominent in 2017.

Commentary

IN 2016, there are four main ways that states have tried to use cyberspace to either raise the level of security in cyberspace, or affect the security stance of other states. First, to misquote Clausewitz, states are increasingly using cyber as an extension of policy by other means. Russia was accused by the Office of the Director of National Intelligence and Department of Homeland Security in October 2016 for interfering with the US presidential elections.

The agencies charged that the Russians hacked into the computers of the Democratic National Congress (DNC), and then leaked the emails to WikiLeaks to discredit the Democratic candidate, Hillary Clinton, whom they thought would be less favourable to Russian interests. This episode provides an interesting twist to what is considered to be the critical information infrastructure (CII) in any given state.

Cyber As A Tool of Influence

Typically, states see CII to be more technical in nature and in fields like transportation, communications, and finance, but now they also need to view the media, electoral and political system as a CII, which needs to be protected against interference from other states who want to influence opinion and decision making.

Singapore is vulnerable to these information operations, given that it has a democratically elected government, and has seen an increasing number of “news” websites commenting on Singaporean issues.

Second, states around the world are increasingly looking to implement strong surveillance laws with regard to cyberspace. China approved its new Cybersecurity Bill in November 2016, with more stringent rules requiring companies to provide data to the Chinese government upon suspicion of wrongdoing. The bill also requires businesses’ domestic data to be stored on Chinese servers and this data cannot be transferred overseas without state permission.

The United Kingdom has also passed the Investigatory Powers Act 2016 giving the state broad ranging powers that allow surveillance to be conducted on a large scale. It is only a matter of time before more states adopt such sweeping legislation on surveillance in cyberspace.

Singapore should be concerned as an aspiring technology hub and international data storage centre, with Singaporean companies and Singapore-based multinational corporations alike owning data that could be subject to other states’ laws and surveillance. There will be more pressure placed on technological companies to provide information and data to states.

Corporations may also have to concede on some dearly-held principles to do business in a foreign state, or forgo business opportunities in that state altogether. Therefore, Singapore needs to consider the economic impact if it were to consider enacting similar legislation.

The Desire for Backdoor Access

Third, states increasingly want back doors to be built into the security of commercially available software, or for access to private data that has been secured by businesses. In the case Apple vs FBI last year, the state, represented by the FBI, brought Apple to court to compel it to help unlock the encryption of a deceased terrorist’s phone. Apple refused to do so, arguing that this would create a backdoor, and would make all iPhones vulnerable to malicious hackers.

Given the failure of the United States in getting Apple to unlock a terrorist’s phone, it may be difficult for Singapore, as a small nation, to compel large corporations like Apple to tweak encryption technology to help with its law enforcement efforts. In the wake of terror attacks this year, France and Germany are also pushing the European Union to adopt a law that would require software companies to make encrypted messages available to law enforcement. The right to privacy has thus come under much pressure in the past year even in Western democracies that were previously known for their liberal views.

Singapore has to determine if its security concerns outweigh the privacy of its citizens. It is not a given that Singaporeans will always choose security over privacy. Attitudes towards the balance between privacy and security are in flux, and laws should ideally reflect the societal attitudes.

State As Protector Of All Data

Fourth, some states appear to be offering cybersecurity protection to private enterprises. In September 2016, Ciaran Martin, the head of cyber at the United Kingdom surveillance agency GCHQ, proposed erecting a government-maintained firewall against malicious hackers. The primary goal of the move is to secure government websites and critical infrastructures against hackers, but in his comments, Martin said it could be expanded to include private companies as well.

While this move naturally raises privacy concerns about governments holding and securing the data, the overall security gain for small and medium enterprises (SMEs) who are concerned about the cost of implementing an effective cybersecurity programme may tempt some of these enterprises to entrust their data or systems to a government-maintained firewall.

States should however be aware of the additional risk in assuming responsibility for cybersecurity of SMEs. While this move may bring SMEs up to a minimum standard, a government cloud, with multiple SME eggs in one basket, would be a prime target for cyberattacks, and any breach or breakdown would result not only in financial losses, but also in reputational and political damage.

2017 And Beyond: Implications for Smart Nation

State intervention in cyberspace is not a new thing, but the tightening embrace of cyber issues by the state can be quite disconcerting and worrying to individuals and business. This is especially true for individuals who fiercely guard their privacy, or those who fear giving states too much power over its citizens. This may well lead to a restriction of fundamental liberties. States need to realise that the increasing Orwellian nature of state behaviour in cyberspace reduces the confidence of all users of cyberspace.

Given the increasing stewardship role of states in cyberspace, there should be appropriate discussion over who will provide the role of ombudsman to the state, and if there is a danger of overreach into the personal lives of people. There is thus also a need to define how information is secured, while protecting both personal and enterprise privacy.

This has implications for Singapore as an aspiring Smart Nation. The state will be responsible for a massive amount of data about its citizens, and any misuse of this data could erode trust in the agencies using the data. There are consequences for expanding the role of the state in cyberspace, and these consequences may not be conducive for the growth of both the society and the economy.

Eugene E G Tan is an Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg