DEFENDING CYBERSPACE: AGENDA FOR ACTION

By
Zahri Yunos and Ahmad Nasir Mohd Zin
National ICT Security and Emergency Response Centre (NISER)

(This article was published in The Star InTech on 5 February 2004)

Information and Communications Technology (ICT) has pervaded national economies, social activities, politics and defence of countries around the world. While all these new technologies allow for enormous gains in efficiency, productivity and communications, they also create new threats and vulnerabilities to those who harbour bad intentions. The same infrastructure that we utilise to transmit information also creates unprecedented opportunities for criminals, terrorists and hostile foreign nation-states.

With viruses and worms as well as hacking tools becoming the latest weapon of choice, we cannot afford to be complacent. Protecting the Malaysia's critical information infrastructures and Malaysia's "e-sovereignty" against cyberattacks should be of grate concern to us all.

We need to outline a national program in order to address the nation's ICT security issues in a comprehensive and effective manner. Malaysia needs a "cyberdefence agenda" to systematically identify the offensive and defensive measures required to defend the country against cyber attacks from individuals, groups, organisations or countries.

Formulating an all around defence from all angles and possibilities can be achieved by considering the following fundamental questions: -

- IF Malaysia is under cyber attack, what should we defend? What must Malaysia need to do to protect herself?

- HOW should we defend? If Malaysia needs to counter cyberattacks, how is the country going to do it? One needs to remember that offensive actions are also a form of defence.

- HOW to make our country prepared to cyberattacks? How should this be integrated into the overall Malaysia defence planning?

We need a comprehensive offensive and defensive capabilities to support our strategic agenda and ensure our "e-sovereignty" is protected.

Some of the examples below may not be total solutions, but may give some ideas on the capabilities that we need to develop.

National Cyber Early Warning System

What can Malaysia do to avoid being a victim of cyber attacks?

We need cyberattack early warning because of the difficulties in identifying and assessing a sophisticated cyber attack. We need a system that combines proactive and reactive incident response capabilities, and at the same time provides 24x7 active monitoring of critical networks from a centralised network monitoring centre.

The system also must be able to provide necessary alerts, carry out an analysis and respond to these alerts.

Awareness Programme

Many are glad with the efforts by the Malaysian ICT community, whether the government or private sector, to raise awareness on information security to a wider public.

These efforts need to be continued until a significant portion, if not all, of society are aware on the importance of these issues.

Information Assurance

The cyber defence strategy should also place a strong emphasis on making sure that critical systems are secured and handled by Malaysians themselves.

One of its most important provisions would be to encourage critical agencies to only buy software that has been certified as being secured, a move that is likely to encourage suppliers to improve the security of their products. The Common Citeria for Information Security Evaluation (ISO15408) can be used for this purpose.

Qualified Information Security Professionals

Qualified information security professionals are important considering the kinds the threats we are facing. There is a possibility that bugs, trojan horses and other sorts of security risks are lurking just beyond our nation's cyber-boundaries. We need to develop information security professionals urgently to ensure the security of our cyberspace.

R&D Centre

Our cyber defence strategy should also include the creation of a centre to study information security and related threats. This could be a joint public-private sector programme to improve the security of the Internet.

Internet security is going to become a greater issue and cannot be be left to just isolated programmes. Researchers scattered throughout the nation should be grouped together under one roof.

Business Continuty Management Standard

The government must make it compulsory for critical public and private sector orgnasiations to widely adopt business continuity management standards. This is to provide effective contingency solutions in order to ensure continuity of business at organisational and national levels in case of a disaster.

These organisations should also conduct risk assessment to help identify their critical security needs, assess their operations and systems against those needs and implement security improvements identified through the risk assessment process.

International CERT Collaboration

Engaging in “cyberdiplomacy” may be a good idea. As with traditional diplomacy, cyberdiplomacy is the interaction of duly appointed representatives of states, international organisations and other such international actors.

The formation of regional Computer Emergency Response Teams (CERTs) such as Asia Pacific CERT, in which Malaysia is a member, is a good example of such interaction, benefiting members through voluntary information-sharing of common cyberthreats.

Adoption of Best Security Practises

With our growing dependence on information networks and the rapid changes in network technology and threats, it is critical for organisations to adopt the best security practices such as implementing an information security management system.

While there is often discussions and debates over which particular practices might be in some way “best”, effective practices and policy templates are recommended for both governments and private sector oprganisations.