S. RAJARATNAM SCHOOL
OF INTERNATIONAL STUDIES
A Graduate School of Nanyang Technological University

RSIS COMMENTARIES

No. 210/2013 dated 12 November 2013

# Securing Cyberspace: Whose Responsibility?

By Senol Yilmaz and Kah Kin Ho

## *Synopsis*

*Besides the ongoing vandalism by Anonymous on websites in Southeast Asia and beyond, cyberattacks can pose serious threats to national security particularly when critical infrastructure is targeted. There is need for private-public partnership to secure cyberspace.*

## *Commentary*

THE CURRENT defacements of websites of governments and businesses are a great nuisance to the victims. However, Anonymous, the network of hackers behind these defacements, declared its intention to create more than just nuisance. In a video published last week, the network threatened to attack the financial sector of Singapore to “cause financial loss”. It remains to be seen whether Anonymous is able to carry out cyberattacks that would result in significant financial damage.

The fact, however, is that critical infrastructure – whether in the finance, transport, energy, or utilities sector – is highly vulnerable. In 2012 for example, the so-called Shamoon virus caused severe disruptions by wiping out data from thousands of computers at Saudi Aramco, the largest oil producer in the world. Allegedly carried out by Iran, a state-actor, it took the company two weeks to recover from the attack.

### Critical infrastructure vulnerabilities

It has been demonstrated that when critical infrastructure is attacked severe disruptions can follow. Further aggravating this situation is that more and more machines connect to cyberspace and become remotely controlled. These include control systems of gas and oil pipelines. In the not too distant future, even more devices will be interconnected ranging from those critical for national security as well as household goods and cars. When targeted jointly in a mass attack, even private consumer goods could turn into a national security threat.

Given the likely increase in vulnerabilities governments worldwide agonise over the right approach to making cyberspace more secure.

From governments’ point of view, protecting critical infrastructure poses two difficulties. First, in many countries, the operation of critical infrastructure as well as the physical and intangible components of cyberspace are held in private hands. Due to private ownership, governments often do not exercise immediate operational control.

Even standard-setting for the Internet is not always carried out by national governments, or inter-governmental bodies, but in open standards organisations such as the Internet Engineering Task Force, where governments have limited say.

Second, governments and the private sector have divergent interests: Governments on the one hand are concerned with ensuring national security while maintaining or creating an environment conducive for economic activity.

The private sector on the other hand has as its main objective making profits and serving shareholder interests. In terms of security, it does what it deems “enough” which may not necessarily be sufficient. In general, every extra dollar spent on security decreases corporate efficiency and shareholder value in the short-term. Incentives to invest in additional security measures are often only recognised once perpetrators have successfully compromised systems. This can be too late in the case of a serious cyberattack that may cause substantial damage.

**Government lead or private sector starring?**

In the context of assigning roles, two diametrically opposing views have emerged. The first argues that corporations have made huge efficiency gains through the computerisation of operations. For example, banks can operate their business more efficiently by allowing their customers to make e-transactions from their homes without interacting with a clerk. Similarly, utilities providers do no longer send staff to manually activate valves or switches located afar from central operation sites.

Rather, the same operation is commanded remotely from a machine, with minimal human action. For these reasons it is argued that the private sector should not only reap the efficiency gains of such automation and computerisation but also share the burden of hardening the infrastructure on which they depend.

The opposing view puts forward that securing the nation is one of the most fundamental tasks of governments. Nobody would expect the operator of a hydroelectric power station to protect its dams against ballistic missiles from adversaries. It is argued that no other standard should apply to figurative cyber-missiles that could result in similar damage.

**Framework for PPP: collaborate, facilitate, regulate**

Arguably, it would be reasonable to share the burden of protecting cyberspace in public-private partnership (PPP). However, there is no magic formula for assigning the roles that governments and the private sector should assume. The culture of governance differs substantially between countries ranging from very little public sector involvement to heavy regulation. Nonetheless, a three-pronged framework could help in this endeavour: there is need for collaboration, facilitation and regulation.

First of all, close collaboration at all levels is crucial. Exchange of information and best practices, or collaboration in screening and analysing malicious internet traffic between Internet Service Providers and governments’ Computer Emergency Response Teams (CERTs) can reduce cyberthreats.

Secondly, governments can facilitate the implementation of cybersecurity measures by providing reliable guidelines and by creating the right incentives. Investments in additional measures could be awarded tax breaks and low interest loans could be provided to companies that invest in the resilience of their systems. Furthermore, governments could consider cybersecurity measures that are in place when granting contracts to businesses.

Last but certainly not least, cybersecurity will likely not be achieved without any regulation at all. Obviously, corporations tend to loath being regulated since regulation can be burdensome and inhibit profit-making. However, governments can develop regulation in close cooperation with the private sector. Richard Clarke, former Special Adviser to the US President for Cyber Security, suggests “smart regulation” is also possible: regulatory end-goals are defined but the best avenues to reach such goals are co-developed with the private sector.

Equally important, legislative processes need to be accelerated to provide timely guidance to narrow the gap between ill-boding technological advances and regulation. The faster governments react, the less the chance of damage.

Admittedly it is a difficult task to balance the interests of governments and the private sector. However, close public-private partnership can prevent mere cyber-nuisance from transforming into a national security threat and finally lead to a win-win situation: an environment conducive for economic activity in a secure nation.

*Senol Yilmaz 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. Kah Kin Ho is Head of Cyber Security Business Development, Global Cyber Security, Cisco Systems.*