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

RSIS COMMENTARIES

No. 209/2012 dated 8 November 2012

Preventing a Digital Pearl Harbour: Panetta's Key Recommendations

By Caitríona H. Heinl

Synopsis

Many states are grappling with the burning question of how best to defend a nation from cyber attack. US Secretary of Defence Leon Panetta recently outlined key best practices in the United States for what is a universal problem.

Commentary

IN AN ADDRESS to the business community in New York, Defence Secretary Leon Panetta captured the mind with images of a "cyber Pearl Harbour". He depicted cyber terrorist attacks as destructive as 9/11 resulting in national paralysis, panic, simultaneous virtual and physical attacks on critical infrastructure, and real-life physical destruction and loss of life. In painting these scenarios he also outlined the gravity of cyber threats for the citizens of the United States and for its economy.

Panetta asserted that cyber attacks are "every bit as real" as terrorism and nuclear weapons proliferation. "Foreign cyber actors" already probe critical infrastructure networks in the US, targeting national transportation and chemical, electricity and water plants. While his doomsday scenarios of destruction and mass casualty are hypothetical and might sound exaggerated, cyber attacks are also considered a Tier 1 threat in the United Kingdom and cyber defence one of the top priorities of the European Defence Agency.

Call for further action

To protect the US, Panetta called for comprehensive cybersecurity legislation, enhanced public-private collaboration, cohesive public sector coordination, and training of expert "cyberwarriors". These four key recommendations are not unique to the US and are of universal application across the Asia Pacific and Europe.

The first calls for timely implementation of cybersecurity strategies and comprehensive legislation such as the Cybersecurity Act of 2012. Disconcerted that the "bipartisan" bill has fallen "victim to legislative and political gridlock", Panetta asked for the business community's support. He argued that for the necessary level of protection, comprehensive cybersecurity legislation is required.

Secondly, while waiting for such legislation to come into force, the US government will continue to work with the private sector. Given the multidimensional nature of cybersecurity, the public and private sector must cooperate. Equally, a recent European Parliament report emphasised the crucial role of complementary cooperation.

Collaboration between government departments and agencies, law enforcement, the intelligence community, the private sector, research institutes, academia and international organisations is critical. Future innovative and pragmatic policies will very likely stem from such forums providing for stakeholder coordination. Working with industry will stimulate technological innovation and the creation of new software systems to protect critical cyber networks.

This, however, poses a challenge as the public and private sectors are not always willing to exchange information. Trust and confidence-building exercises are required. At EU level for instance, the European Parliament has recommended establishing a permanent dialogue.

In addition, many incidents in the private sector are not reported because of the sensitive nature of the information and fear of possible damage to company reputation. Voluntary or obligatory disclosure of known attacks could better inform authorities and assist in formulating a stronger response. The European Parliament has also proposed that in return for such disclosure through “a rapid information exchange system”, authorities could guarantee anonymity.

Overcoming the “classic stove-piping problem”

Thirdly, Panetta cited a broad whole-of-government approach as an effective model for the US. This is significant since there is uncertainty in many other countries over which government departments and agencies are responsible for cybersecurity, while in others there is “turf war”. Likewise, at the regional EU level, too many agencies are involved. Cyber issues can straddle numerous government ministries and agencies such as those responsible for foreign affairs, home affairs, criminal justice, ICT, innovation or defence. Government departments may be unable or unwilling to exchange information, even between themselves.

The European Parliament has proposed horizontal coordination between and within EU institutions on cybersecurity. Other initiatives include coordinating bodies for enhanced governmental coordination, taskforces comprising members from the ministries concerned, and/or allocating lead responsibility to a national cybersecurity coordinator.

In the case of the UK, the Office of Cyber Security and Information Assurance was established to support the Minister for the Cabinet Office and the National Security Council, and to provide strategic direction, coordinate action and work closely with lead government departments.

Investment in skilled cyberwarriors

Finally, Panetta proposed that “the most important investment is in skilled “cyberwarriors”. However, many governments do not have adequate financial resources to attract “the best and the brightest” who are often attracted to “lucrative returns of the dark side”. Even “hiring the hackers” is difficult with inadequate resources. Expertise as well as cross-cutting knowledge, skills and capability is unavailable.

With cuts in government spending, especially for defence, vital investment in cybersecurity might be affected. This is particularly the case in the US and in the EU. The Pentagon had previously announced insufficient resources to defend the country “adequately from concerted cyber attacks”. Significantly however, Panetta has confirmed that the Department of Defence is investing over USD3 billion annually, and that “even in an era of fiscal restraint”, it is continuing to increase key investments in cybersecurity. The UK has implemented a four-year £650 million programme, and EU member states have been urged to increase defence expenditure for cybersecurity and cyber defence.

Drawing on Panetta’s proposal for investment in “skilled cyberwarriors”, countries, including those in Asia, can begin training a new generation of cyber experts and create talent for both home and abroad. The UK and US intend to “produce many thousands of people with this expertise over the next few years”. In the UK, the first eight universities have been awarded “Academic Centre of Excellence in Cyber Security Research” status to provide top quality cybersecurity graduates, support the government’s cyber defence mission and drive innovation.

Many states have yet to develop comprehensive cybersecurity strategies. As national, regional and international frameworks are created in the near future, the international community is closely observing such new initiatives and models of best practice so that they may be applied and built upon.

Caitríona H. Heinl is a Research Fellow at the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.