PacNet
Number 38

Pacific Forum CSIS
Honolulu, Hawaii

May16, 2017

The ARF moves forward on cybersecurity by Brad Glosserman

Brad Glosserman (brad@pacforum.org) is the executive director of Pacific Forum CSIS. This analysis draws on the CSCAP Cybersecurity Workshop that he co-chaired in Indonesia on April 5; the report from that meeting, along with key findings, agenda, and participant list, is available here.

The Wannacry virus that attacked computers around the world last week is one more reminder of the growing threat posed by vulnerabilities in cyberspace. Over 100,000 networks in over 150 countries were infected by the malware; the actual ransoms paid appear to have been limited, but the total cost of the attack – including, for example, the work hours lost – is not yet known. Experts believe that this is only the most recent in what will be a cascading series of attacks as information technologies burrow deeper into the fabric of daily life; security specialists already warn that the next malware attack is already insinuated into networks and is awaiting the signal to begin.

Cyber threats are climbing steadily up the list of Asia-Pacific security concerns. Experts reckon that cyber crime inflicted $81 billion in damage to the Asia Pacific region in 2015 and the number of such incidents is growing. Online radicalization and other content-related issues pose expanding threats to the region, challenging national narratives and in some cases undermining government legitimacy and credibility. The networks and technologies that are increasingly critical to the very functioning of societies are vulnerable and those vulnerabilities are being distributed as regional governments are more intimately connected and more deeply integrated in economic communities. One recent study concludes that an ASEAN digital revolution could propel the region into the top five digital economies in the world by 2025, adding as much as $1 trillion in regional GDP over a decade. This growth and prosperity are threatened by proliferating cyber threats.

Fortunately, regional governments are cognizant of the dangers and taking action to address them. The ASEAN Regional Forum (ARF) first tackled cyber issues in 2012 and it developed a work plan to promote cooperation and build confidence in 2015. ASEAN launched its Ministerial Conference on Cybersecurity a year later, and Singapore has begun a SG$10 million cyber capacity building program.

Central to the success of those projects is confidence building measures (CBMs). The complexity of information networks makes it hard to identify with confidence the sources of misbehavior. The fact that cyberspace is borderless and vast means that malicious behavior is difficult to prevent and its effects can quickly spread far beyond national boundaries and intended targets. Effective prevention, mitigation and response measures demand working relationships among governments and other key players. This is only possible if there is trust among them.

There is no shortage of ideas on how to build confidence among states in cyberspace. ASEAN has identified 11 areas in its work plan and the ARF has developed a list in its work plan. Other organizations, such as the Organization for European Security Cooperation and the European Union, have also developed CBMs and they can be borrowed when appropriate.

The success of such efforts depends on several prerequisites. First, there must be an accurate assessment of a country's own cyber capabilities. It is impossible to cooperate if countries do not know the limits of their own and their partners' capacity. The Australian Strategic Policy Institute (ASPI) has developed a report, *Cyber Maturity in the Asia Pacific*, which draws on publicly available information to offer an annual assessment of national cybersecurity programs. While the ASPI initiative is valuable, it would be better for countries to prepare their own analyses. The process would promote dialogue across key constituencies (government, businesses, and technical), increase official awareness of capabilities and shortcomings, and lay the foundation for conversations between governments. Uniform assessments would also standardize vocabularies and facilitate communication, ensuring that words have the same meaning across constituencies.

The second requirement is the establishment of trusted channels of communication among all stakeholders. This requires not only the identification of those stakeholders, but confidence that information shared will be respected and protected. That "respect" includes confidence that when a party tries to communicate, the call or email will be answered in a timely fashion. Regular and routine dialogues among stakeholders will also build trust, familiarity, and routines that will facilitate problem solving when crises occur.

A third requirement is the standardization of expectations, formats and procedures. Baselines are needed so that countries can assess standing and capabilities relative to others and so that partners will have realistic expectations of them. Templates can be developed to address how to share information, how to request assistance, and how to pursue legal action.

Despite the broad consensus in the Asia-Pacific region on the need to collaborate to address cyber threats, regional governments have been slow to implement CBMs, even those that have been identified by the ARF. This reflects a number of factors. In many cases, information technology and security is either too new, evolving too rapidly or seemingly too peripheral to core concerns to command the attention of decision makers. Among security planners, cyber issues can seem distant from priority national security concerns or too

specialized. Some of these problems can be remedied by adopting a mindset that recognizes that cybersecurity is a strategic, rather than a technical, problem. Similarly, effective cybersecurity demands a whole of government approach, rather than one that leaves it to specialists. Finally, effective cybersecurity measures should be seen as confidence building and trade enhancing measures. As in the strategic trade control debate, governments and businesses need to abandon the view that these measures are designed to slow their development and see them instead as means to spur growth: countries and businesses will be more inclined to trade with partners that have secure cyber technologies.

While numerous institutions and organizations address cyber threats and challenges, the ARF is especially well suited to lead in this area. ARF efforts build on the ASEAN model of cooperation, one that is inclusive and respects diversity, an especially important consideration in a region where countries have a wide range of capabilities, limitations and needs. The ARF is cognizant of the need to adopt solutions tailored to regional and national circumstances and member governments understand well how to work collaboratively to raise collective capacities.

The ARF is working toward that end. Member governments look set to create a permanent cybersecurity inter-sessional meeting (ISM), a move that would underscore the ARF's commitment to focusing on cyber issues as well as create a forum for substantive work to address cyber challenges. The ARF commitment is critical as many experts believe that the Asia Pacific could lead global efforts to develop regional cybersecurity regimes with its sensitivity to diversity and sovereignty, and the state of national and regional IT infrastructure – the Asia Pacific can more easily build in security than can more developed economies. After a fitful start, the region and the ARF appear to be mustering the political will to meet those challenges. After the news of last weekend, and the fears that Wannacry is only the first of many new threats, it is about time.

PacNet commentaries and responses represent the views of the respective authors. Alternative viewpoints are always welcomed and encouraged.