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

RSIS Commentaries

RSIS presents the following commentary Plugging Cyber Warfare Governance: Asia Should Act Now by Elina Noor. It is also available online at this link. (To print it, click on this link.). Kindly forward any comments or feedback to the Editor RSIS Commentaries, at RSISPublication@ntu.edu.sg

---

No. 151/2013 dated 15 August 2013

Plugging Cyber Warfare Governance: Asia Should Act Now

By Elina Noor

Synopsis

While academics debate whether cyber warfare is even possible within the traditional notion of war, three realities need to be confronted. Thus far silent on the issue, Asia must now contribute to the evolution of laws to govern cyber warfare.

Commentary

IN THE past century when states were pushed to fight wars, they would do it the old-fashioned way: by amassing troops and weapons on a country's borders, flying overhead and dropping bombs, and launching surprise attacks underwater. Land, air, and sea were – and remain – the conventional military domains for war.

Increasingly, however, cyber space is emerging as a complementary domain of, and a perfect extension to, warfare. If the "virtual wars" of Bosnia and Kosovo in the 1990s allowed for remote-controlled wars from a safe, ensconced distance, technological advances now and in the future will progressively afford the luxury of quicker and cheaper keystroke wars.

Guns for keyboards

In cyber space, a virtual realm with no natural or geographic borders, and constantly dynamic packets of data routed from one node to another, the world really is flat. It is also anonymous since identity verification

is not yet required and can be masked through complicated routing patterns.

For technologically less-advanced states, cyber warfare levels the field by offering asymmetric benefits in cost and effect. Stuxnet, considered a sophisticated malware that was arguably the first to be weaponised and released with intent to destroy critical infrastructure in peacetime, cost only several million US dollars. Now that the code has been deconstructed, it will be cheaper to replicate or improve upon for future attacks. Even North Korea, perceived by the outside world to be deprived in so many ways, is believed to have thousands of trained hackers to launch cyber attacks.

In fact amassing force can be cheap in the digital age. A botnet army recruiting unsuspecting, compromised devices can be marshalled at minimal cost and with zero logistics to propagate malware. A state in conflict with another might tap into the patriotic, nationalistic fervour of its citizens by crowd-sourcing cyber attacks.

What makes the prospect of cyber warfare disturbingly distinct from the other domains of war is how blurred the civilian-military line is due to how integrated cyberspace is in daily life. More and more nations are wiring their critical infrastructure – from the electricity grid to waste management and air traffic control – to cyber space.

Legal ambiguities

Additionally, with the exception of some tweaking, much of the software marketed to the military is typically based on the same platforms available commercially. Even if a system is isolated from the Internet – "air gapped" – the user remains the weakest link so a security breach could happen just by an employee plugging an infected USB device into a computer drive.

A 2011 study, "Cyber security and cyber warfare: Preliminary assessment of national doctrine and organisation" estimated at least 33 states that include cyber warfare in their military planning and organisation. Given the limitations of open-source data, the possibility of undervaluation, and the likelihood that this number will only keep growing, there is a need for a set of regulations to govern the developing conduct of cyber operations as a means and method of warfare.

International law, broadly framed, offers markers to the rules of the road. There is also an analogical corpus of laws related to other unconventional weapons – nuclear, biological, chemical, and radiological – that provide insight into how existing international laws might apply to cyber warfare.

Of course, questions would need to be resolved, such as whether the provisions on peace and security within the UN Charter would apply to non-state actors, or whether they would treat economic collapse of a nation brought about by cyber attacks equally to physical destruction by kinetic weapons.

Asia should act now

As things stand, however, Asia – despite having some of the most connected systems and populations in the world – is curiously quiet in this unfolding discussion. The challenges of war in or using cyber space affect any and every country that pins reliance of its critical infrastructure on the millions of nodes in cyber space. The region must actively participate in, contribute to, and influence the conversation now as norms are being shaped. Otherwise it risks being left out at later stages when laws have crystallised.

Security and defence cooperation among ASEAN and its partners should be expanded to tabletop exercises and simulations of cyber warfare. The concept of interoperability in military affairs is even more of an imperative in the virtual realm; so regular cooperative exercises should increasingly become the norm.

Given that cyber space cuts across the public/private divide, effective policy solutions must embrace and leverage on the technical skills of the private sector. The two "industries" often not only speak different languages but also past each other. A comprehensive cyber warfare stratagem must involve the private sector at policy roundtables and in simulations, whether at the Track One or Track Two level.

Conversely, private sector-organised IT security forums across the region should include strategic policy

discussions to encourage not only meaningful exchanges but also coherent approaches to managing cyber warfare.

Finally, there should be greater engagement of the legal community within the defence ministries around the region as well as of multilateral organisations such as the International Committee of the Red Cross in exploring and elaborating the sets of rules that should govern the evolution of cyber warfare. Track Two institutions could, for example, act as intermediary in engaging with these parties within their respective countries to formulate national positions on these issues which would, in turn, clarify interactions and negotiations at the regional and international levels.

Elina Noor is Assistant Director for Foreign Policy and Security Studies at the Institute of Strategic and International Studies (ISIS), Malaysia. She contributed this specially to RSIS Commentaries.
