Draft notes

‘Jaw Jaw’ is better than ‘War War’: International Security in Cyberspace

Remarks by Paul Meyer to Cyberbudapest 2012, October 5, 2012

I have drawn the title of my remarks to this panel from Winston Churchill’s famous maxim concerning the desirability of dialogue over destruction in the conduct of relations between states. As a great war-time leader, it was not that Churchill was a pacifist, but he did see the merit of trying to resolve disputes first on the basis of dialogue and mutual understanding, before having recourse to armed force. As a former diplomat, I share the predisposition to look at possibilities for conflict prevention through the application of diplomacy and the peaceful settlement of disputes.

As a result, when I survey the current environment for international cyber security I am troubled by the relative dearth of preventive diplomacy and the apparent dominance of militarized approaches to achieving security in cyber space. Given the particular nature of cyberspace, its ‘global commons’ character and its extensive and predominant civilian application, there is reason to question an assumption that it represents just another domain for armed conflict and offensive operations. Unlike the terrestrial or other environments, cyberspace is a human creation and the activity within it is subject to human decisions as to the extent of cooperation or conflict that should prevail in this environment. We all know that there is a heavy presence of non-state actors within this new environment, but as this panel is focused on the ‘international security’ dimension of cyberspace, I will concentrate on the state actors and the future of inter-state behaviour.

We are still at an early stage in addressing the issue of inter-state behaviour and frankly the future course of events in cyber space could go either way on the cooperation-conflict spectrum. As has frequently been the practice in the past, when the international community has been confronted with the question of how to handle a new development with implications for international security, the world has looked to the leading powers for guidance on the path to follow. Sometimes those powers have been able to cooperate to forestall militarization or weaponization of sensitive environments. One can think of the treaties on the Antarctic, outer space, the seabed, environmental modification and the WMD prohibition agreements such as the BWC and CWC. In other situations, weaponization was allowed to proceed, but with various limits and restrictions placed on these systems and their deployments, as witnessed by the many arms control accords of the past century. And in yet other aspects, behaviour is unregulated formally, but reflects shared norms which have developed over time – e.g. nuclear deterrence.

In this context of international security regime development, the United States traditionally has played a leading role, often being the major architect of new arrangements and then seeking support for these from other actors. The cyber space realm has seen some initial path-breaking policy work by the U.S. in the form of its *International Strategy for Cyberspace* released by the White House in May 2011. This strategy recognises the tendency of some governments to seek “to exercise traditional national power through cyberspace”, while calling for the development of internationally agreed “norms for acceptable state behaviour through cyberspace”. The Obama administration however has yet to be able to translate this progressive vision into actual processes which yield substantive results. Currently this administration is distracted by electoral considerations and is not giving thought to issues of high policy. Critics might also protest that the administration’s apparent involvement in the deployment of the “Stuxnet” and “Flame” cyber weapons, renders it a poor standard bearer for that “peaceful and just interstate conduct” in cyberspace that its strategy proclaims.

In light of the huge stake civil society has in secure and sustainable access to cyberspace, we should not accept a *laissez faire* approach being taken by states with respect to international cyber security. This environment is too precious to leave it to the cyber generals (or captains) to “safeguard” as they see fit. In the absence of a great power champion willing to convene a global forum on norms for responsible state behaviour on cyber security, to whom can civil society look for some action on this front? At present there are only a few options out there which might bring some discipline and purpose to what hitherto has been a disjointed debate. One of these is for regional security organizations to look seriously at developing such norms and associated measures as to provide some agreed framework in which to conduct cyber operations. The Organization for Security and Cooperation in Europe (OSCE) has recently initiated a working group “to elaborate a set of draft confidence-building measures (CBMs) to enhance interstate cooperation, transparency, predictability and stability and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs”. The diverse membership of the OSCE and its successful history in the development of CBMs in the political-military field augurs well for this enterprise, but it is very early days.

At the universal level, and a central feature of cyber space is its global nature, the United Nations has begun to address itself to the challenge of international cyber security. It has done so largely through the establishment of a Group of Governmental Experts (drawn from a representative set of some 15 states) to consider issues relating to security in cyber space. An initial consensus report in 2010 recommended the development of “confidence building, stability and risk reduction measures”. A new GGE has got underway this year and is due to report back to the UN General Assembly by the fall of 2013. These GGEs operate on the basis of consensus however and it is by no means certain, especially as the governmental experts move beyond formulating general platitudes to grappling with specific measures that agreed recommendations will be forthcoming. Concerned civil society should be monitoring closely these processes and seeking input to them. Civil society should also be maintaining pressure on governments to ensure that serious diplomatic engagement to devise the norms for responsible state behaviour is sustained. The diplomacy of international cyber security cooperation has lagged far behind the cyber actions of military establishments and it is time for a reassertion of the principle of the civilian control of the military in determining what sort of state conduct in cyberspace we wish to see.