"Outer Space and Cyber Space: War or Peace?"
Remarks for Canadian Pugwash Group Conference
Canada's Contribution to Global Security Halifax, N.S, July 23-25, 2017

My title was inspired by Tolstoy's classic, but with the suggestion that the existence of states of war or peace entails a degree of choice. It was and is within the capacity of humankind to choose paths that lead to one or the other result. For centuries armed conflict has raged in the domains of land and sea. The dawning of the last century introduced a new battle space in the form of air warfare. We have become depressingly accustomed to violent clashes in all three terrestrial domains that provide regular fodder for our media audiences.

There are however two other environments which have up to now escaped the grim fate of "weaponization" and overt use of force although they are both experiencing a militarization, that if left unchecked, will be a dark harbinger of actions to come. It is still possible, in my opinion, for the international community to choose the future nature of these environments and via the application of diplomacy and advocacy engage in conflict prevention.

The first of these special environments I would like to address is outer space; an environment of human use for over half a century and one that has enjoyed a unique status in international relations. This status flows from a treaty that in my view stands as one of the great achievements of preventive diplomacy: the Outer Space Treaty of 1967. This underappreciated international agreement, the golden anniversary of which we celebrate this year, granted outer space the status of a "global commons" in which no sovereign claims could be made and for which any use should be for peaceful purposes and in the interests of all humankind. The peaceful orientation of the treaty was reinforced by provisions that prohibited the stationing of WMD in orbit and the militarization of the moon or any other celestial body.

The use of outer space has grown exponentially since the OST was concluded. Today some 1500 active satellites owned by 60+ countries or consortiums orbit the earth and provide humanity with a wide array of services crucial for our contemporary well-being. While the "peaceful purposes" nature of the OST has been interpreted as allowing for non-aggressive military uses of space, this domain has so far escaped the "weaponization" that could lead to armed conflict in space. The bulwark against this development represented by the OST is only as good as state practice in support of it. The current climate of deteriorating East-West strategic relations, the advent of alarming threat assessments and escalating, belligerent rhetoric to match is not conducive to maintaining a benign operating environment in space free from the threat of attack. The revival of long dormant anti-satellite weapons (ASAT) programs further fuel mistrust and increase the probability of a space arms race - an arms race that the international community has long pledged to prevent.

Although with 105 states parties the OST would seem to have firm support, the relative neglect of its 50th anniversary by leading space powers is disturbing. It suggests a tendency to dilute legally-binding constraints on a nation's conduct in favour of unrestricted freedom of action. As an early multilateral accord, the OST lacks any provision for meetings of its states parties, a standard feature of contemporary international accords. Civil society has suggested that it would be most fitting for the first ever meeting of states parties of the OST to be held this year to celebrate its 50th anniversary and provide a venue for discussion on its current condition and future needs. Neither the three depositary governments of the treaty (US, UK and Russia) nor any of the 105 parties have taken the initiative to organize such a gathering. Governments seem to have abdicated their responsibility to uphold the principles and commitments of the OST at the very time these elements of peaceful cooperation are being challenged.

It would be timely for the wider stakeholder community (the private sector and civil society) with an interest in continued peaceful activity in outer space to advocate for active measures by their governments in support of the legal regime for outer space and the promotion of peaceful international cooperation in this unique environment.

I would now like to turn to another special environment, one that also is in danger of being transformed into yet another battleground. This environment shares many of the features of outer space in terms of utility for humanity's prosperity and welfare as well as its essential vulnerability to attack and malevolent action. It is however a human and not a natural creation and its exploitation is of an even more recent time period, barely a quarter of a century.

I am referring to cyberspace, most saliently represented by the Internet, but encompassing the vast network of computer systems that facilitate so much of human endeavor in the contemporary world. The Internet now boasts over three billion users, double this number if one includes the increasingly smartphones in the hands of so many around the globe. It would be hard to exaggerate society's dependency on cyberspace and the Internet and yet this was a platform originally intended for exchange of information amongst a trusted group of scholars and scientists; hence the low level of security incorporated into its design.

Despite the enormous global impact of the Internet, little in the way of international governance of it has been agreed. An environment overwhelmingly owned and operated by the private sector and civil society, states have belatedly turned their attention to it. In doing so efforts at sovereign control have increased, while attempts to forge an international consensus on norms for responsible state conduct have been halting. In the absence of an early foundational international agreement, akin to the OST, cyberspace is still something of a "Wild West" when it comes to subjecting in to a cooperative international regime.

While desultory and disjointed discussions have occurred in various forums over the last decade, state action has proceeded apace largely unchecked by any international constraints. In the last few years armed forces around the globe have established cyber security units, staffed with "cyber warriors" and increasingly acknowledging that offensive as well as defensive capabilities are being developed. This on-going militarization of cyberspace is only the most visible indication of state capabilities as the origins of government exploitation of cyberspace resides in intelligence agencies and has advanced under a thick mantle of secrecy.

A policy of secrecy has not prevented revelations as to damaging state conduct in cyberspace. A Rubicon of sorts was crossed in 2009-10 with the exposure of the "Stuxnet" worm, arguably the first cyber weapon that brought about physical destruction of its target. This sophisticated cyber attack was aimed at disrupting Iran's nuclear program, by sabotaging the operations of centrifuges at its main uranium enrichment facility. Although no state has ever acknowledged responsibility for launching this weapon, evidence points to the US as prime actor. One can only wonder if the question of whether to authorize this first weapon had been put to Internet users in America what the results of the vote would have been.

The revelations of ex-NSA contractor Edward Snowden also demonstrated the extent to which governments were engaged in massive surveillance of communications of their own citizens. The cyber campaigns mounted recently by states or their proxies to influence elections in democratic countries are further evidence of malicious activity. Unfortunately, the intelligence agencies that have developed potent cyber "exploits" to penetrate target computers, have proven incapable of safeguarding these secrets and thus have contributed to the onslaught of cyber criminals as in the recent "Wannacry" ransom ware attacks.

Negative state conduct has regrettably far outpaced diplomatic efforts to develop a cooperative security paradigm for cyberspace. At the UN, a series of Groups of Government Experts (GGE- normally 15 to 20 national representatives that meet behind closed doors to study emerging issues and generate consensus reports) has provided the principal mechanism for consideration of cyber activity in the context of international security. These GGEs have produced reports in each of 2010, 2013 and 2015 that have gradually set out norms and measures for the elusive responsible state behavior in cyberspace. The latest report, for example, has called for restraint measures that would exclude critical infrastructure and computer emergency response teams from being targets of cyber attack. These worthy recommendations, remain however just that, unless states actually move to adopt and implement them. There is a danger that the GGEs become convenient vehicles for states enabling them to appear to be responsible players, while in fact having little impact on their actual conduct.

As with outer space, it is time for the wider stakeholder community to speak up and put pressure on their respective governments to take real action to bring about peaceful international cooperation in cyberspace. It is a domain too important to

leave to the generals (or to Lieutenant Henry Hotspur of Cyber Command) if humanity wishes to continue to avail itself of the Internet's vast potential for good.