Op-ed by Paul Meyer and Daniel Stauffacher
“Disarmament negotiations for the Cyberspace are needed”
Neue Zürcher Zeitung, Monday, 23 July 2012 (translation)

The world is facing a new challenge - a modern arms race with no visible weapons and identifiable actors, which is characterized by a growing number of known and hidden attacks on websites of government agencies or infrastructures. It often remains unknown, who ran these attacks, whether by governments or non-state actors. The fact is that new technologies provide in cyberspace a new generation of offensive weapons. One of the major powers could soon decide to use cyberspace as a battlefield in order to decide an inter-state conflict. And with such, the vital question would be answered, whether an exclusively peaceful use of the cyber-space will continue to be possible or whether we are approaching its definitive militarization.

No matter in which direction the journey goes, the consequences for international security will be substantial. The diplomatic and military elites of the leading cyber-powers are therefore required, as soon as possible, to develop a common approach, how to behave in the future in this unpredictable and dangerous environment. Should Governments not soon develop coherent strategies for international cooperation in this area, they could very soon be faced with a fait accompli.

The inter-state dimension of security in cyberspace is a new challenge, and its importance is generally not yet fully understood. So far, the discussion on international cyber-security has primarily focussed on the problems of crime, cyber-terrorism and the role of non-state actors. In the fight against criminals and terrorists, it was easier for States to find common ground for cooperation among themselves. But now it’s about their own behaviour - especially in cases of conflict.

The States must therefore in their consultations go beyond issues of criminal and terrorist activity in cyberspace and try to define now also the limits of so-called "unacceptable state behaviour" in cyberspace. Currently, there is no general agreement about what is meant with "acceptable" or "responsible" cyber-activity by a State. In such a grey area of international law states are largely free to decide on their own what constitutes an “acceptable” action. It is clear, however, that recently States carried out or supported activities which, while not expressly prohibited, can have a destabilizing effect.

From an international perspective, we are still at a very early stage in the development of rules for cyberspace. There are still widely divergent
concepts, how to define legitimate government action in cyberspace. There are those who see cyberspace as a “global commons” and emphasize the need to protect it from threats. On the other side are those who see cyberspace as another area to carry out warfare.

A key challenge for government policy makers will be to determine how much cyber-activities are already governed by existing international political and legal regimes. If one could subsume cyber operations under existing international legal norms, the international community would certainly have already won a lot. However the development of a common understanding by legal scholars, such as how the existing standards can be applied to cyber-operations is progressing slowly. There is a risk that because of this vacuum in the meantime the still largely peaceful nature of cyberspace could be compromised by government actions of offensive nature.

For military cyber operations substantial resources are being made available. This is in contrast to the limited resources that are being used to develop binding and acceptable guidelines for such operations. The U.S. Department of Defense estimates that more than thirty countries have or are in the process of creating cyber units within their armed forces, similar to the Pentagon’s own cyber command established in 2009. According to its mission statement: “US CYBERCOM is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense’s information networks and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries”.

Although reference is made to ensuring compliance with existing law, it is evident from this doctrine that the U.S. will not hesitate to deny an opponent the use of the cyberspace, with offensive or defensive means. How such a denial would occur, the internal rules that would apply and the possible implications for international security are not discussed in this doctrine. But it is precisely these issues that the public urgently needs to discuss. And here the international community is clearly lagging behind the military developments. There are, however some encouraging indications that such discussions are being launched.

There are signs that at the UN, more importance is being given to the question of responsible state behaviour in cyberspace. A first contribution to this debate was the report of the UN Group of Governmental Experts
(GGE) on “Developments in the Field of Information and Telecommunications in the Context of International Security”. The formation of this group is an initiative of Russia within the framework of the UN General Assembly, which for the first time pointed to the impact of information and communication technologies on the international security architecture. The expert group recognized for the first time officially that states develop techniques for cyber-warfare and espionage, and recommended further discussions between States in order to reduce societal risk and protect critical infrastructure, national and international.

The UN Group of Governmental Experts is being convened again in 2012 with a mandate to prepare a further report. Should this group, which also includes the five Permanent Members of the UN Security Council, produce a consensus report, this may have a major influence in shaping the ‘rules of the road” for cyber security at the international level.

In the framework of the Organization for Security and Cooperation in Europe (OSCE), of which Russia is also a member, government officials are presently preparing in an informal working group under American Chairmanship, a first set of confidence building measures (CBMs) on a regional basis, to minimize the risks of misunderstandings and escalation in the cyberspace.

The publication in May 2011 of the "International Strategy in cyberspace" by the US White House represents another milestone in the discourse on international security in cyberspace. The Obama administration acknowledges in the report for the first time the danger that might come from uncontrolled cyber-operations: “Cyber security threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace”. The report also recognizes that norms for states in cyberspace are missing. The American strategy set as a goal to resolve this shortcoming. The US wants to help bring about a consensus on what constitutes "acceptable state behaviour in cyberspace." The opinion of the United States, that standards must be developed in a multilateral context, is an important signal in which direction the American diplomacy in the future might go.

The British government has recently also taken a leadership role on these issues, by convening in November 2011 a Conference on cyberspace. At this conference, the participating States recognized, that their operations in cyberspace must be in line with existing international law and traditional norms of interstate behaviour. The London Conference will continue in 2012 in Hungary and in 2013 in South Korea. Such meetings are necessary
and laudable; they do not replace however the multilateral diplomatic processes.

If more security is achieved through international cooperation in cyberspace, sooner or later real agreements on the behaviour of states must be negotiated. In a first phase, such agreements are likely to have only the character of legally non-binding instruments. Fortunately, there are now signs that other states have also recognized that there is a political vacuum, which must be addressed. Because it takes more than just a few general principles and visions, but concrete suggestions as to what is meant by a permitted or not permitted state behaviour in cyberspace.

Russia and China, two other leading cyber-powers have also begun to develop standards. They submitted in September 2011 to the UN General Assembly a proposal for an “International Code of Conduct for Information Security”. The chief undertaking of this voluntary code would be a commitment of states “not to use Information and Communication Technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies”’. Moscow and Beijing, further suggest confidence-building measures (CBMs). This could be a first step in the development of rules in cyberspace without having to go the very complicated way of negotiating an international agreement.

But it will not be easy to find a consensus on the content of such a code of conduct. The central prohibition on “hostile activities” “threats to international peace and security” and the proliferation of “information weapons or related technologies” introduces terminology that is open to wide interpretation. Similarly, what one state might view as a “disturbance” or “sabotage” of its cyberspace. When assessing the possible steps of a preventive diplomacy for the security and peace in cyberspace, the international community can rely on the experience with confidence building measures (CBMs) in the area conventional weapons.

First confidence building steps could be, for example, the publication of national cyberspace-specific doctrines and multilateral consultations. One could add the joint observation of "military cyber manoeuvres", common situation reports and the establishment of communication links for consultations in case of conflicts in cyberspace. In addition, countries could formally renounce the first use of cyber weapons. At the international level also a catalogue could be worked out, which enumerates the measures tools for self-defence that are legitimate.
All this would need to happen in a as global context as possible, because the
Internet itself is a global phenomenon. It is worth noting that today, that
even the U.S. Defense Department explicitly wishes confidence building
measures to prevent an escalation in cyberspace. Cyber-diplomacy is in
great need to catch up with the military developments. Confidence-building
measures must become a priority for governments.

Paul Meyer is a former Canadian Ambassador to the UN Conference on Disarmament in
Geneva. Today he teaches at Simon Fraser University in Vancouver. Daniel Stauffacher is
a former Delegate of the Swiss Federal Council and Ambassador of Switzerland. He is the