Cyber activities are acquiring a growing military dimension and, it is widely recognized that after land, sea, air and outer space, cyber has become the fifth potential theater for international conflicts. In some instances, the use of cyber for military purposes could be considered as an armed attack as defined by the United Nations Charter. Studies have been published highlighting the interdependence between cyber activities and a possible weaponization of outer space. Also the reliability of nuclear weapons as a deterrent can be seriously affected by cyber attacks. Eminent personalities of the European Leadership Network (a non-partisan think tank based in London) jointly underlined, in a recent statement, the risk that "cyberattacks from state or non-state actors can lead to the theft of nuclear materials or sabotage to a nuclear facility, false warning of a missile attack, or the intrusion into nuclear command and control systems."

The most notable episodes of an international use of cyber as a weapon were an attack in 2007 which swamped the websites of Estonia and, in 2010, the use of the "Stuxnet" virus against the Iranian Uranium enrichment unit. It is noteworthy that neither Iran, i.e. a UN member, nor Estonia, i.e. a Nato and EU member, invoked the respective defense clauses foreseen by those organizations. More recently, the dispute over Russian interferences during the US presidential campaign has added a new political dimension to the potentially destabilizing effects of cyber activities. The cyber world, though providing innumerable benefits, has become a double-edged sword and a potential instrument to destabilize international peace and security leading to possible catastrophic consequences. Many states have been prompt to militarize their cyber activities by establishing ad hoc structures integrated into their military chains of command and fully dedicated to cyber defense and offense.
However, states have not been as swift in seeking new norms to prevent a cyber-arms race and in addressing unprecedented situations that are becoming ungovernable. NATO must be credited for having published, soon after the cyber-attack against Estonia, the Tallinn Manual, a text that contains a selection of the already existing international norms applicable to cyber warfare. This includes the prohibition of the use, or threat of use, of force and the principle that cyber weapons can only be used for self-defense. It also stresses the equivalence between a cyber-attack and a kinetic attack. However, the Tallinn Manual is not a legally binding text (not even for NATO) and identifying already existing legislation applicable to cyber warfare can only be a first step towards a more advanced process which should take into account the specific peculiarities. Namely the fact that: 1) the offensive use of cyber creates an unprecedented problem of attribution of responsibility for cyber attacks. Their authors cannot be clearly identified, and non-state actors play at the same level as states. 2) Cyber operators, use their instruments of war during office hours against enemies often located thousands of kilometers away. Even if belonging to the military and wearing a uniform, they cannot be considered “combatants” as defined by humanitarian laws. 3) Because no blood is shed and no immediate human suffering is evident, cyber attacks are less visible to media and public opinion. 4) The verification and transparency of any international deal on cyber would be much harder to execute than in the case of conventional or mass destruction weapons. In spite of these peculiarities and difficulties, some useful “cyber specific” steps have been taken. At the domestic level states such as the US and the UK, introduced ad hoc provisions and national strategies on cyber activities.

Through its 2016 Global Strategy for Foreign and Security Policy, the European Union launched a process of closer cooperation on security and defense that includes cyber activities. In December 2017, 25 EU States decided to activate a Permanent Structured Cooperation (PESCO) on Defense that includes projects dedicated to cyber. A first batch of these projects includes the establishment of a European Cyber Information Sharing Platform and of European Cyber Rapid Response Teams. At the bilateral level, Russia and China finalized a cyber-security pact in 2015. In the same year, the US White House published a fact sheet on the visit of the Chinese President containing a chapter dedicated to cyber security bilateral cooperation. At the regional level, in December 2013, the Organization on Security and Cooperation in Europe (OSCE) introduced a set of confidence building measures (CBM) dealing with communications and information sharing, programmes and strategies relevant to cyber security. A second set of CBMs aimed to reduce the risk of tensions arising from cyber activities was established in 2016. Additional efforts, focusing on stability measures and responsible state behavior are being considered. At the multilateral level, the UN Secretary General established four successive Groups of Governmental Experts (GGE) focusing in particular on new confidence building measures tailored to cyber security. These include the principle that “States should not knowingly allow their territory to be used for internationally wrongful acts using ICT”. A number of UN General Assembly resolutions have been approved and a draft code of conduct initiative, led by China and Russia, has also been tabled. Unfortunately, the last meeting of the GGE held in 2017 closed without a consensual report and thus without concrete guidance for the future. At the G7 Taormina Summit, last year a “Declaration on responsible behavior in cyberspace” was endorsed by Heads of States and Government. It provides for the establishment of new measures “voluntary and applicable only in peace time” specifically tailored for cyber activities. The G7 also addressed the controversial question of attribution by declaring that “States cannot escape legal responsibility for internationally wrongful cyber acts by perpetrating them through proxies.”
Confidence building measures and codes of conduct are often preliminary steps leading to the establishment of legally binding norms. We are not there yet. The momentum of all the existing initiatives must be maintained but more ambitious goals must be pursued. A “bottom up” process should be initiated starting with the establishment of a wider network of national legislations and strategies on cyber security as the basis on which to construct an international norm. More countries must follow the example of China, Russia and the US in establishing bilateral cooperation on cyber security. The measures adopted at the regional level by the OSCE and those suggested by the G7 group, both of a voluntary nature, should acquire a politically binding configuration. A future G7 ad hoc text on cyberspace should be adopted by the leaders themselves and not merely “endorsed” by them. At the UN, the GGE approach should not be a substitute but rather a vehicle for achieving more advanced measures such as: States to prohibit their territory from being used for wrongful cyber acts and holding full responsibility for such acts. States should report to the UN on national norms and other relevant cyber security texts. The UN should establish a repository of such domestic norms and guidelines. By including two cyber projects in the first batch of PESCO initiatives, the EU shows that it “means business” in developing its cyber security related activities. The challenge is now to implement those projects within the complex mechanism of the Permanent Structured Cooperation. By so doing the EU will give an impulse to the establishment of international rules on cyber activities.