A NEGOTIATION ON CYBER WARFARE

CARLO TREZZA[1]

to be published by SPRINGER: THE IMPACT OF CYBERSPACE

Abstract In spite of the growing the risk that cyber capacities could be used as military tools no international agreement has been finalized so far to prevent a cyberwarfare involving sovereign states as well as non-state actors. States have different conceptual approaches and priorities when approaching this subject and discussing definitions. There are additional peculiarities. The possession and use of cyber weapons capacities are not visible. The author of an attack cannot be clearly identified, and non-state actors can play at the same level as national states. The operators of such weapons can hardly be included in the classical legal category of "combatant".

Most countries have already established cyber structures integrated into their military chains of command and fully dedicated them to cyber defense and cyber offense.The cases of the US, Nato,European Union and the United Nations.Cyberwarfare has not yet acquired a legal status of its own in spite of the fact that after land, sea, air and outer space, cyberspace has become the fifth domain in which states can confront each other militarily.States have not even started to negotiate any sort international regulation.The Tallin Manual on the International Law applicable to cyber warfare has no international legal value but has the merit of having established some fundamental principles.It indicates that the norms applicable to cyber are the same as those applicable to the other types of weapons and in particular the International humanitarian law.

[1] Address correspondence to the author:

Nothing prevents the international community from considering cyberwarfare also in a preventive mode, and to craft cyber-specific rules prohibiting cyber instruments capable of provoking catastrophic consequences. A general prohibition of possession and use of cyber offensive capabilities would ideally be the preferable solution but we are no where close to such a solution. An uncontrolled cyber incident could act as a shock absorber to prevent a conflict from escalating;it could also become a trigger for a wider confrontation that the international community cannot risk. The problem of how to address the security implications of a cyber world will be with us for the years to come. Better to address the issue in a preventive mode rather than subsequently to a possible cyber confrontation.

Key words cyberwarfare, conventional weapons, weapons of mass destruction, the Shanghai Cooperation Organization, "cyber combatant",USCYBERCOM,NATO strategic concept,ENISA (European network and Information security Agency),Tallin Manual on the International Law applicable to cyber warfare,International humanitarian Law, cyber confidence building measures,Obama, Mogherini.

Text

The cyber world has existed for more than three decades; in paralel, a military/security dimension has also been developed. It could possibly lead to a confrontation between states and to a cyber "arms race". In spite of this clear and present danger and of the risk that cyber capacities could be used by terrorist groups, no international agreement has been finalized so far to prevent a cyberwarfare involving sovereign states as well as non-state actors. In his foreword to the latest UN report on cyber activities the UN Secretary-General (UNSG) noted that “The benefits (of cyberspace) are enormous, but these do not come without risk. Making cyberspace stable and secure can only be achieved through international cooperation, and the foundation of this cooperation must be international law and the principles of the UN Charter". (1)The UNSG was correct in indicating that the existing international norms must be the basis to achieve stability and security in cyberspace. Implementing laws already in existence is necessary but may not be sufficient to attain those goals; therefore, additional rules, better tailored to the military/security cyber environment and to its peculiarities, are to be pursued.

It is difficult to establish the category to which cyber weapons belong. Are they to be considered conventional weapons or Weapons of Mass Destruction (WMD)? The distinction between these two categories, although artificial, is fundamental: only nuclear, chemical and biological are considered as WMDs. Cyber, by exclusion, would, therefore, fall into the category of conventional weapons. This has legal consequences. According to UNSC resolution 1540 (2) which is a legally binding resolution under Chapter Vll of the UN Charter, only the proliferation of WMDs is a threat to international peace and security. Thus, the proliferation of cyber weapons and cyber technology, at least from a legal stand, does not represent a threat to international peace and security. Their possession is not prohibited, and their use and threat of use are only subject to the general international rules on warfare.

The issue of cyberwar is further complicated by the fact that states have different conceptual approaches and priorities when discussing definitions. The Shanghai Cooperation Organization members defined cyberwar to include dissemination of information "harmful to the spiritual, moral and cultural spheres of other states"(3). What they fear is that freedom of information and the penetration of political or religious ideas through the cyber networks might destabilize national societies and become a mortal threat to the survival of their regimes. This is not a far fetched hypothesis. Let us only consider the role played by electronic devices in the hands of demonstrators during the so called "Arab Spring".

Western countries have different priorities. They view cyberwar as causing effective physical damage and injury to their military assets and strategic infrastructures. They are more open to freedom of speech and information and in principle, they oppose limitations to the circulation of political and religious ideas via the cyber network. And yet, episodes in the West of whistleblowers being prosecuted, investigation agencies asking cyber companies to reveal their codes, indicate that even Western countries feel vulnerable to a total liberalization.

There are additional peculiarities. The possession and use of cyber weapons capacities are not visible. The author of an attack cannot be clearly identified, and non-state actors can play at the same level as national states. The tradition of starting a military confrontation through an official war declaration is no longer applicable, and it is more and more difficult today to establish if and when a war situation starts. The operators of such weapons can hardly be included in the classical legal category of “combatant”; they rather belong to a new profile that can be defined as “armchair warriors.”. As the pilots of UAVs, the cyber operators use their instruments of war during office hours against enemies located thousands of kilometers away. These remarks don't want to be derogatory for the servicemen involved in such activities which require strong technical, juridical and psychological preparation, but they are not comparable to the risks and stress of direct combat.

Addressing and improving the present rules governing cyber warfare is not an easy task. Most countries have already established cyber structures integrated into their military chains of command and fully dedicated them to cyber defense and cyber offense. In many ways the gene is already out of the bottle; “militarization” is a fait accompli: all modern armed forces rely heavily on computers and would be totally paralyzed should they renounce them.

In the United States of America, President Barack Obama stated in 2009, that digital infrastructure was a “strategic national asset”(3) and in May 2010 the Pentagon set up its Cyber Command (USCYBERCOM) in Fort Meade, Maryland..According to the 2015 US National Security Strategy “cybersecurity requires that long-standing norms of international behavior – to include protection of intellectual property, online freedom, and respect for civilian infrastructure” should be respected.(4)

The NATO strategic concept and subsequent NATO summit and ministerial declarations recognized the urgent task of protecting the Alliance's information and communication systems and the necessity to integrate cyber defense into NATO’s defense planning. These concepts were further elaborated at the recent NATO summit in Warsaw in July 2016 where it was decided that cyber defense will continue to be integrated into operational planning and Alliance operations and missions. NATO commitment to act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law in general, was reaffirmed. NATO also addressed the question of an ad hoc new legislation indicating its preference for “voluntary international norms of responsible state behavior and confidence-building measures regarding cyberspace”.(5)

The original response of the European Union (EU) to the development of a cyber threat was prevalently of a civilian nature. It took place through the establishment of ENISA (European network and Information security Agency). Globally, the EU strives for an open and secure cyber realm, in which cyber issues are firmly anchored within the framework of human rights, rule of law and international law. The cyber threat was addressed in the new EU Security Strategy which was announced in June 2016 by the EU High Representative for Foreign and Security Policy, Federica Mogherini (7). The language adopted contains substantial policy indications within the EU as well as with external partners. Reference to norms which should regulate this new chapter of international security will hopefully be developed in greater detail in the future.

Cyberwarfare is not a prerogative of the Euro/Atlantic region. Other areas and countries such as Russia, China, India, North Korea, Israel and many others are active in developing military capabilities in this field. In general, countries that have acquired such capabilities are reluctant to negotiate international norms which could compromise the advantage they have reached.

So far, the world has not experienced cyber attacks of the scale and effect allowing the international use of force. Even in the acutest known cyber episodes such as the use of Stuxnet in Iran, which temporarily paralyzed an Iranian nuclear enrichment installation and the cyber-attack against Estonia which in 2008 swamped the websites of Estonia including parliament, ministries, newspapers. In these two cases, neither Iran nor Estonia invoke Chap VII or art 51 of the UN Charter; neither did Estonia as a member of both of NATO and the European Union, invoke the NATO and EU defense clauses (Nato Art. 5 of the North Atlantic treaty; EU art 42 and 222 of the Lisbon Treaty).

Cyberwarfare has not yet acquired a legal status of its own in spite of the fact that after land, sea, air and outer space, cyberspace has become the fifth domain in which states can confront each other militarily. All these domains have been subject throughout the years to some kind of normative regulation. Even in the case of outer Space, which preceded cyberwarfare as the latest addition to new warfare theaters, an international treaty was finalized only ten years after the launch of the first Sputnik.

Nothing similar has happened yet in the cyber world. As of this moment, States have not even started to negotiate any sort international regulation. This does not mean that the issue has not been addressed. Since 1998, there have been annual reports by the UN Secretary-General to the General Assembly containing the voluntary information of UN Member States on their cyber activities8). The attention of the UN became more focused when a Group of Governmental Experts (GGE) was established. Its mandate was to examine the existing and potential threats from the cyber-sphere, as well as possible cooperative measures to address them. This group has now been renewed four times, and its main focus has been the establishment of voluntary non-binding norms and confidence building measures, international cooperation and capacity building. In the latest edition of the GGE report, a clear priority was given to the effects of cyber-attacks against critical infrastructures and terrorism.(9)

Subsequent to the cyber-attacks in Estonia in 2008, NATO established a Cooperative Cyber Center of Excellence in the Estonian capital of Tallin, in order to enhance NATO’s cyber defense capability. The center produced the Tallin Manual on the International Law applicable to cyber warfare which was authored by 20 leading international legal experts(10) In spite of the fact that the Manual has no international legal value, it has the merit of having established some fundamental principles. According to the Manual, the general principles of international humanitarian law apply to cyberwarfare both in the conduct of war (Jus in bello) and during the process leading to war (Jus ad bellum). This implies that the prohibition of the use or threat use of force enshrined in article 2 of the UN Charter also applies to cyberwarfare. This also indicates that cyber weapons can only be used for self defense or with the authorization of the UN Security Council under chapter VII of the UN Charter. The Tallin Manual also establishes the principle of equivalence between a cyber-attack and a kinetic attack: “A cyber operation constitutes a use of force when its scale and its effects are comparable to non cyber operations rising to the level of a use of force”(11). It is not questionable that in a war situation (Jus in bello), the norms applicable to cyber are the same as those applicable to the other types of weapons and in particular the International humanitarian law. Therefore, general principles of necessity, of proportionality between offense and response, the protection of civilians, and the clear military advantage expected from an operation are also applicable to cyber weapons.

The general norms mentioned so far apply to an already existing conflicting situation. Nothing prevents the international community from considering cyberwarfare also in a preventive mode, and to craft cyber-specific rules prohibiting cyber instruments capable of provoking catastrophic consequences. In an ideal world, new ad hoc norms should be devised to deal with the strategic and humanitarian implications of cyberwar and cyber weapons. Initiatives in this field have been initiated by academics and experts. But the bold step of passing from academic and political deliberations to full-fledged negotiations has not yet been taken. As in other similar scenarios, countries that have reached a technological advantage are reluctant to tie their hands in a negotiation.

But unless codes of conduct, limitations, and reductions are negotiated, a destabilizing arms race in cyber power is unavoidable. Every state will pursue what it believes is its immediate interest, without considering the general long term implications.

What are the options we have today? A general prohibition of possession and use of cyber offensive capabilities would ideally be the preferable solution. We are no where close to such a solution. A prohibition limiting the offensive use of cyber weapons, meaning that countries would be allowed to possess but not to use such a type of weapon, could be a more realistic option. However, recourse to such a type of arrangement is normally motivated by humanitarian reasons, i.e. to avoid causing unacceptable harm to the civilian population and to reduce the suffering of combatants. In past experiences, the humanitarian approach was closely connected to "graphic" episodes of cruelty which had an impact on public opinion and mobilized the NGOs. The humanitarian consequences of a malevolent use of the cyber weapons have not been fully evaluated so far, and thus the establishment of a coalition of likeminded countries spearheading the negotiation of an international ban, as was the case for anti-personnel landmines and cluster munitions, has not been achieved so far.

A mechanism specifically dedicated to the risks connected with a cyberwarfare has yet to be invented. In the meantime, as a first step, preliminary measures of transparency and confidence building, as indicated by the UN Group of Governmental Experts must be set up(12). A clearer overall picture of the risks connected with cyberwarfare is also necessary. The work done by UN experts in this field is encouraging. An uncontrolled cyber incident could act as a shock absorber to prevent a conflict from escalating. Nonetheless, it could also become a trigger for a wider, global weapons confrontation that the international community cannot risk. The problem of how to address the security implications of a cyber world will be with us for the years to come. Better to address the issue of a cyber escalation in a preventive mode rather than subsequently to a possible cyber confrontation.

References

1)Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.UN General Assembly DocA/70/174 July 22/2015

2)Resolution 1540 (2004) adopted by the Security Council at its 4956th meeting, on 28 April 2004 first paragraph:"Affirming that proliferation of nuclear, chemical and biological weapons, as well as their means of delivery, constitutes a threat to international peace and security",

3)Shanghai Cooperation Organization Agreement among Member States in Cooperation in the field of Ensuring International Information Security "Art 2 para 5.Yekaterinburg 3/12/2008(unofficial translation)

4)The White House:Office of the Press Secretary May 29, 2009:Remarks by the President on Securing our Nation's cyber infrastructure.

4)The White House:National Security Strategy February 2015 page12

5)Nato Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 Para 70/71

7)"A Global Strategy for the European Union", Brussels June 2016 Page 21

8)Based on UN General Assembly Resolution A/Res/53/70 such reports have been submitted by a limited number of Member States

9)On 23 December 2015, the UN General Assembly unanimously adopted resolution 70/237 which welcomed the outcome of the 2014/2015 GGE and requested the Secretary-General to establish a new GGE that would report to the General Assembly in 2017.

10)Tallin Manual on the International Law Applicable to Cyber Warfare. New York, : Cambridge University Press 2013

11)Tallin Manual Rule 11: Definiton of the use of force

12) Para five of UN Genera Assembly documentA/70/174 22 July 2015 :"Confidence-building measures increase cooperation and transparency and reduce the risk of conflict. The Group identified a number of voluntary confidence-building measures to increase transparency and suggested that States consider additional ones to strengthen cooperation. The Group called for regular dialogue with broad participation under the auspices of the United Nations and through bilateral, regional and multilateral forums."

Author’s short biosketch

Carlo Trezza was Italy's Ambassador for Disarmament and Non Proliferation and Ambassador to the Republic of Korea. He chaired the Conference on Disarmament in Geneva, the UN Secretary General's Advisory Board for Disarmament Affairs and the Missile Technology Control Regime (MTCR).