# NATO and its Cyber Defence

By: Catherine Stella Schmidt
Political Scientist and author

Cyber Space is a territory, even though it has less limit than the physical one, it can yet be tackled and under control.
This significant step, not only scientifically but also politically and militaristically is plausible.
Only it has to be defined conceptually; recognized legally; regulated by the International Laws and Treaties.

Harnessing the Cyber Space is not a simple task that could be accomplished effortlessly and by a single NATO Member. It is a security pillar which requires inexorable discipline and engagements from all NATO Member States.

It will be crucial that the North Alliance Treaty Members to join forces by sharing capabilities, intelligence, science, Cyber technology and Military to build a stronger defence in order to tackle the perennial crisis of Cyber Space.

In the complex runaway world,
if only we could place the jurisdiction boundaries on the cyber space of each global Nation then we might be able to establish the Rule of Law that could actively govern the Cyber Peace and Security.

Evidently one of the essential steps that NATO, perhaps should consider to take, is to strategize its Cyber Defense policy more assertively yet audible to the world.

Added to that in the West, particularly in US and Europe, we have to apply a comprehensive measures in the Cyber Security fronts by:

- Providing a regular training to our Federal and Military personnel
- Mobilizing our communities and civilians with the essential Cyber education and Awareness tools
- Facilitating environment and resources for academics/Scientist to develop the high-caliber applications which could protect our Cyber Space and National Security.

Simultaneously NATO, while maintaining its original framework, should reset and prioritize its Security and Operational concepts in the twenty-first century.

Further recommendations will include:

• To outline a far broader framework on Cyber-Defence which could encompass a new regulations for counter-measures; while having all the means of defense, and the right to defend its Allied available on the table- if one of its Member States be targeted by any categories of Cyber invasion.

• While all Western countries are dealing with the Cyber threats on a daily basis, NATO and its policy-makers have to develop an immediate and far more assertive Cyber Defence strategies which should guide our defencee during the time of peace as well as the provision for counteroffensive in the eve of Cyber conflict or war.

• It has also to expand its structures by establishing the Cyber Defense Allied Unit, which could bring all the Members to work, coordinate and synchronize more closely with the Organization, in order to maximize NATO’s Cyber Defence.

• And finally, NATO Members have to initiate a step for establishing an International Cyber Cooperation Corps which would have the authority and the mandate to act and observe the International Cyber Security Treaties and Laws among the world Nations.

With the multiplied threats lurking from every frontier, the Militarization of our Cyber Space will be an indispensable, the foremost required measure that NATO Members have to concentrate and implement henceforth.