Commission : OSCE - Organization for Security and Co-operation in Europe Council

Subject : Towards a strategy of cooperation between the OSCE and the European Union to counter terrorism and cyber warfare ?

Author : United States of America

In recent years, cyber attacks on a serious scale have become a matter of concern to states, due to the threat they can pose to national security, but also a potential foreign policy and military tool to be added to existing options in their arsenals. While international law is still struggling with defining norms on state actions in cyberspace, the latter is now increasingly viewed as a fifth domain of warfare. The definitions surrounding 'cyber war' and 'cyber defense' are still widely debated, and indeed have become a growing topic for international legal jurisdiction, along with governments and international organizations. Cyber attacks and cyber crimes are increasing in number and sophistication across Europe. This trend is set to grow further in the future, given that 30.3 billion devices worldwide are expected to be linked to the Internet by 2025.

The United States of America has militarized the response to cyber-attacks through its Cyber Command (United States Cyber Command / USCYBERCOM), launched in 2010 and bringing together the cyber components of the US Navy, the US Marine Corps, the army and air force into a unified command. USCYBERCOM is one of the largest cyber defense organizations in the world. In 2011, the US Department of Defense (DoD) adopted the 'Strategy for operating in Cyberspace' which rests upon five strategic initiatives: cyberspace will be treated in the European Parliamentary Research Services (EPRS) Cyber Defense in the EU Members' Research Service similar to air, land, maritime and space domains.

The United States of America' overall goal is to fight against cyber terorism. In order to respond to this threat, Snowden leaks have offered information about the US Monster Mind programme, designed for automated response to cyber attacks against the US. The Pentagon has also increased spending on cyber operations ($26 billion over the next five years) and pledged to build a 6 000 strong cyber force. Besides the development of offensive and defensive cyber capabilities, the US pursues a norm-setting agenda internationally, to set rules about what kind of cyber operations constitute an act of war. Moreover, a 2013 presidential directive instructs the US to aid allies who come under foreign cyber attack.

The United States of America's Department of Defense will employ new defensive methods for dealing with cyber threats; cooperation at national and international levels will be encouraged. Finally, the Department of Defense will focus on developing a pool of skilled personnel and technological innovations. Although predominantly defensive (the Pentagon is said to possess 90% offensive and 10% defensive cyber capabilities), the creation of a strong offensive deterrent has been advocated by high-ranking military officials in the US. The Department of Defense's new cyber strategy does not explain how offensive capabilities might be used or the 'active' cyber defense posture.

The United States of America, willing to cooperate with the European Union to counter terrorism and cyber warfare, stresses the need to raise more awareness on cyber issues at the political and strategic decision-making levels by providing decision-makers with relevant knowledge and information and underlines the need to enhance the awareness of the general public and promote cyber hygiene. Besides, the United States of America reminds the importance of a coordinated approach as well as the development and implementation of effective measures at national level to reinforce the cybersecurity of 5G networks. The US reports and reminds the risk of the increase of

sophisticated robots on the internet, privacy violations, and faster data extraction that can escalate with 5G.

The United States of America welcomes the adoption of additional Cyber Confidence Measures and hopes the best in terms of cyber public awareness campaigns, research and development, and educational programmes, as well as cyber industry and capacity building. Last but not least, the United States's Cyber Command will pursue its efforts to strengthen cyber security and cyber defense dimensions with a view to ensuring that these are fully integrated into the wider area of security and defense.