TECHNOLOGY AND CYBERSECURITY:
HOW THEY AFFECT THE AFFAIRS AMONG THE STATES

Choutea Eleana (MA)
(RIEAS Research Assistant)

First published on Geopolitcs & Daily News - (Greek language)

It is fair enough to describe the 21st century as "Century of Technology and Information". The relationship between political technology and military technology becomes closer as the first produces dual use technology used by the latter. Technological development of a state undoubtedly affects economic and military power in times of war and peace, transforming the world and influencing relations among states

Technology and International Affairs

In the context of international relations, technology plays an important role because of military security in general and especially in the conduct of war. One of the most important international problems associated with technology is cyber espionage and its definition is equally difficult. The definitions given are many, since it is difficult to give a unanimous and commonly accepted one.

The perception of cyber holds many difficulties. Those difficulties have their origins to the complexitivity of factors that affect the cybersecurity. In 2013 at Tallinn Congress in NATO, cyber espionage was defined as "that act committed secretly or by

false intentions and using cyberspace capabilities to collect (or attempt to collect) information for the purpose of transferring them to rival." Paradoxically, there are no technical obstacles to help the states that are victims of these attacks, but legal and political barriers are those that make it difficult for a state to defend itself.

Cyber espionage and Cyber attacks

The fact that a real war among great powers in the modern world is less acceptable makes the preference of other strategies more preferable. There are many different cyber-espionage tools available for states, many of which do not differ from the attacks that one might take on their personal computer, the difference lies on the grounds of a larger scale on a larger scale. Two major trends are related to the modern cyber-espionage of states, which have shaped not only the cyberspace but also the public perception of cyber-espionage and war. The first refers to that cyber-espionage which becoming more and more sophisticated, effective and professional. As far as the second trend is concerned, cyber-espionage is accepted - even preferred - as a way of war, affecting the nature of the conflict between states without replacing traditional means of war. Digital technology has an unexpected impact on cyber-espionage. For example, anyone could have access to the victim's network and handle what the victim sees in real time. This kind of tactical usage, had started in the Cold War when the United States and Russia focused their efforts on collecting secret information. With technology evolving more and more in recent decades, cyber-espionage tools are an integral part of modern military operations.

In recent years, cyber attacks have been reported in government facilities in various countries. One of the most well-known is the cyber attack that Estonia received in 2007, which lasted more than 10 days, with the consequences of the almost total collapse of the energy distribution network, the banking system and telecommunications. Cyber attacks have also grown in Greece since 2007, with more serious attacks on the websites of the Ministry of National Defense and the electronic network of the Hellenic Center for Marine Research in Heraklion, Crete.

However, the technological capabilities of the Internet and the freedom of moving funds are not only exploited by states and companies. It is a good ground for

exploitation by modern organized crime, as its illicit activities, such as the recruitment of new members and further transactions, are facilitated.

How this could be confronted?

Due to the new environment and these special conditions that shape and test prosperity and security, the potential cooperation between private sector with the public should be exploited. This is supported by former US Secretary of State Hillary Clinton. "The problems we face today cannot be solved by governments alone, but through partnerships." At the same length are the statements of European officials saying "Security by definition is cross-sectoral and cross-border. So you have to act externally to achieve internal security and vice versa." Partnership between public and private sector, fall into several categories of activities, such as the exchange of know-how, the information sharing and the execution of projects. This collaboration does not only benefit both parties but also society itself. Acute power - whether as a tool for cyber attacks, interceptions, etc. - either by individual actors or by states - can be addressed through the innovative technologies offered by the private sector and the security offered by the state.