Centre for Economics
and Foreign Policy Studies

EDAM Cyber Policy Paper Series
2017/1

Cyber Security: Understanding the Fifth Domain

June 2017

Can Kasapoglu
Defense Analyst, EDAM

This paper was supported by
Robert Bosch Stiftung

CYBER SECURITY: UNDERSTANDING THE FIFTH DOMAIN

Cyberspace differs from the physical dimensions in which traditional international competition takes place. It is the fifth, novel space for political–military, economic, social, and cultural interactions. Apart from land, sea, air, and space, cyberspace is man-made and depends on electromagnetic spectrum to exist. This complex structure is composed of computers, fiber-optic cables, telecommunications components, critical infrastructures, cyber-personas, digitalized data, and more. Through the fifth dimension, data is exchanged, stored, and modified. Notably, all these transactions rely on the electromagnetic spectrum for operate functioning inter-connected information.

Essentially, entering into the cyber competition is relatively low-cost compared to other domains. State and non-state actors can engage in cyber activities with more affordable investments than that required for launching a space program or operating a power-projecting, blue-waters navy. No territorial ownership or ruling supranational body is governing the cyberspace. There is no disarmament or non-proliferation regimes. Even more importantly, cyber-norms are still taking baby steps. Thus, we are talking about a 'yet shaping' dimension of international affairs.

In the 21st century, societies have become more 'digitalized' in terms of their socio-cultural and economic activities. This trend is coupled with the developments in the military affairs segment, which is getting even more dominated by 'informationalized battlespaces' and network-centric warfare concepts. Furthermore, drastically increasing global connectivity has boosted the information operations aspect of modern warfare. Besides, international competition 'below the threshold of armed conflict' is largely taking place in the cyberspace. In this respect, cyber-related activities range from influence operations to subversive activities.

Terrorism has also found itself a place in the cyberspace. Cyber-terrorism is considered an 'appealing opportunity' for terrorist groups due to low-cost / low-risk, but high-impact and sensational results that could be achieved in short time. In addition, attribution problems in cyber competition remains an incentive for cyber proxy conflict, as well as cyber espionage.

Under these circumstances, applying the core international relations concepts of 'national power', 'national capacity', or 'deterrence' to explain the cyberspace strategic outlook is not easy. The question of how to define and judge cyber power, or decide between two nations' cyber capabilities reflects a complex analytical and even paradigm-building efforts. To find explanatory answers to the abovementioned questions, one would need thorough conceptualizations for each layer of the cyberspace. In fact, such a conceptualization effort is indispensable for adapting to the fifth domain. Indeed, adaptation remains the key way-forward for survival in this new dimension.

Centre for Economics and Foreign Policy Studies

edam

EDAM Cyber Policy Paper Series 2017/1

June 2017

Cyber Security: Understanding the Fifth Domain

Can Kasapoglu
Defense Analyst, EDAM