Centre for Economics and Foreign Policy Studies

edam

EDAM Cyber Policy Paper Series
2017/2

Cyber Warfare:

Between the Future Military Reality and Today's Science-Fiction

September, 2017

Dr. Can Kasapoglu
Defense Analyst, EDAM

This paper was supported by

Robert Bosch Stiftung

EXECUTIVE SUMMARY

Cyber warfare remains a popular phenomenon that still needs robust conceptualization efforts to be better explained in context. While there is a common understanding about traditional segments of war among scholars, say, submarine warfare or chemical warfare, developing such a consensus on cyber warfare does not seem plausible, at least in short term. The differences of opinion in framing cyber warfare is not limited to strategic studies. In order to talk about waging war with a cyber toolkit in the cyberspace, a crystal clear and explanatory understanding of how to prosecute a 'cyber warcrime', and more importantly, how to apply the law of armed conflict to the cyber field must be determined. Furthermore, in order to apply the law of armed conflict and the international humanitarian law to cyber conflicts, first and foremost, one should clarify key terms like 'civilian targets', 'proportionality', and 'the right to self defense' within the relevant framework. Finally, in order to meet the abovementioned criteria, the international community has to come up with a thorough definition of what makes a 'cyber weapon' and what are the expected –non-kinetic and kinetic– impacts.

Even after cyber weapons could be defined and cyber warfare could be conceptualized with a globally shared understanding –noting that the international community is far away from reaching such a consensus at the time being– the very need for avoiding an actual cyber war situation would come into the picture. In doing so, global policy community would require effective non-proliferation and disarmament regimes to prevent a cyber arms race between nations. At this point, some key questions would emerge: Is a cyber NPT regime possible? Which international body would oversee such a regime, and what kind of verification and control mechanisms would be required? Could the world leaders manage to establish an institution like the International Atomic Energy Agency (IAEA) or the Organization for Prohibition of Chemical Weapons (OPCW) to restrict and monitor cyber weapons? The international community also has a long way to go in addressing the abovementioned issues.

While the need for limiting an arms race in cyberspace is becoming even more relevant, many of the world's leading militaries have already started to establish cyber commands within their doctrinal orders of battle. This is a game-changer trend that deserves utmost attention.

This report is prepared as an introduction to cyber war and cyber warfare issues for the academia and professionals working in this field. The first part will explain the determining characteristics of cyber war in detail. Consequent chapters will analyze contemporary and possible future impacts of cyber capabilities on modern militaries' way of fighting their wars. Finally, the report will present its findings in the light of a case study.

Centre for Economics and Foreign Policy Studies

edam

EDAM Cyber Policy Paper Series 2017/2

September, 2017

Cyber Warfare:
Between the Future Military Reality and Today's Science-Fiction

Dr. Can Kasapoglu
Research Analyst, EDAM