Grey Zone Conflicts in Cyber Domain: Nonlocality of Political Reality in the World of "Hyperobjects"

2

Muhammed Can
University of Minho, Portugal

INTRODUCTION

Living in the age of advanced technologies comes with a price: Witnessing exponential growth in artificial intelligence, software-hardware systems and the cyber domain has rendered problems more ambiguous. The vulnerabilities of states, societies and individuals have become more evident thanks to the advent of these technologies. One of the most challenging manifestations can be seen in the grey zone conflicts which state and non-state actors constantly mobilize in order to show their strength. Given the existence of weapons of mass destruction (WMD) and deterrence among great powers, it is roughly impossible to expect great powers to dare overt sabre-rattling, which would eventually lead to total chaos throughout the world. Therefore, grey zone conflicts or political warfare has become both a lesser evil and low-cost option for rival states. As Mazarr puts it, grey zone conflicts consist of "salami-slicing strategies, fortified with a range of emerging area or unconventional techniques from cyberattacks to information campaigns to energy diplomacy" (2015, p.2).

Russia's influence operations and alleged interference in the US elections in 2016, Chinese efforts to shift status quo in the South China Sea, Iran's way of using grey zone tactics via proxies in its immediate vicinity and the pervasive utilization of unconventional tactics by terrorist organizations, notably by the so-called 'ISIS', make grey zone conflicts more significant not only for states but also for laypeople, whose lives are affected by these conflicts along a spectrum of severity. These impacts can be easily discerned in the election process, the perception of reality, diplomatic bargains, unexpected interference by major powers (annexation of Crimea through 'little green men') and information warfare.

It is evident that the cyber domain is a major part of grey zone conflicts. Cyberattacks on the political campaign of Emmanuel Macron, the Russian-backed hackers Cozy Bear and their 'Lisa case' attacks in Germany, the cyber conflict between Russia and Estonia, and Russian influence campaigns in Sweden, Ukraine and Georgia are among the most recent examples of grey zone conflicts in the cyber domain. In the same vein, it is also explicit that these confrontations between rival states have impacted the nature of political realities, which have rendered merely 'virtual' the function of conventional democratic practices – particularly in authoritarian regimes – just as occurred in the post-Soviet landscape (Wilson, 2005).

Apart from being in the midst of these conflicts, political realities have become more ambiguous, which adversely affects states, non-state groups and societies. Moreover, these political realities that are particularly manufactured in the cyber domain have become a nonlocal 'hyperobject', which simply refers to "genuine nonhuman objects that are not simply the products of a human gaze" (Morton, 2015, p.199). In his seminal book, Morton coined the term 'hyperobject' via object-oriented ontology. For

DOI: 10.4018/978-1-5225-9715-5.ch018

him, hyperobjects represent the coexistence of humans and objects and simply correspond to "things that are massively distributed in time and space relative to humans" (Morton, 2015, p.1). Therefore, a hyperobject might be the biosphere, a black hole, uranium or plutonium, or it might be "the very long-lasting product of direct human manufacture", all of which have a plethora of features in common (Ibid). Firstly, hyperobjects are vicious, meaning that "they stick to beings that are involved with them" (Ibid). Secondly, hyperobjects pervade high-dimensional space, and their effects can be found 'interobjectively' in a space that includes interdependence between the "aesthetic properties of objects". Finally, they are nonlocal, meaning that "they involve profoundly different temporalities than the human-scale ones we are used to" (Ibid).

Therefore, this chapter primarily seeks to reach possible answers regarding how the cyber domain of grey zone conflicts affects the political realities on the frontlines. It also attempts to reach an appropriate conclusion to determine possible regulations and existing conventions to counter grey zone conflicts in the cyber domain. Finally, it investigates the reality itself – and its manipulative nature – by putting 'hyperobjectivity' at the centre in the context of political reality.

MODERN GREY ZONE CONFLICTS IN THE CYBER DOMAIN

Grey zone confrontations are not a new phenomenon; they are "a nuanced form of warfare where antagonists seek limited political victories, as opposed to outright military triumphs that would be easier to identify and respond to" (Matisek, 2017, p.2). What makes these types of conflicts problematic is that they technically occur between the lines of peace and war, which is not in accordance with NATO's Article 5 threshold or the UN Security Council's definition of violence of (Echevarria, 2016). In the wake of World War II, major powers have started to use limited force to eschew total disaster. This type of conflict usually comprises diplomatic, information/cyber, military and economic areas (DIME) "to gain influence and leverage or weaken, destabilize, subvert or overthrow governments without resorting to war" (Robinson et al., 2018, p.8).

Grey zone conflicts "have been conducted in the past under such name as 'political warfare', 'covert operations', 'irregular or guerrilla warfare', 'active measures' and the like" (ISAB report, 2017, p.1). The term 'political warfare' can be traced back to 1948, when it was coined by American diplomat George Kennan in a memorandum. He defines it as "the logical application of Clausewitz's doctrine in time of peace." In the broadest definition, political warfare/grey zone conflicts are the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations range from overt actions such as political alliances, economic measures (like ERP – the Marshall Plan) and "white" propaganda to covert operations such as clandestine support of "friendly" foreign elements, "black" psychological warfare and even encouragement of underground resistance in hostile states"(Robertson et al., 2018, p.2). Furthermore, according to the United States Army Special Operations Command (2018, p.2), "political warfare/grey zone conflicts encompasses a spectrum of activities associated with diplomatic and economic engagement, Security Sector Assistance (SSA), novel forms of Unconventional Warfare (UW), and Information and Influence Activities (IIA)".

Keeping that in mind, the characteristic of grey zone conflicts might include (ISAB report, 2017, p.2):

- Cyber, information operations, efforts to undermine public/allied/local/regional resistance, and information/propaganda in support of other hybrid instruments;
- Covert operations under state control, espionage, infiltration, and subversion;