Chapter 8
Collective Cyber Defense:
Legalization of Cyberspace

Mariam Nebieridze
Universitat Regensburg, Germany

ABSTRACT

In the 21st century, activities in cyberspace rose and developed significantly. New security dynamics aftermath of the Cold War have led to a shift in the world's power structures. Non-state actors (corporations, organizations, and individuals) now can reflect strategic global power due to modern information and communication technologies. Collective defense in cyberspace might be more challenging considering the nature of the virtual dimension which accomplishes two factors. They pledge the signatories to resist a shared threat, and as a result, are designed to dissuade possible aggressors. They stand at the nexus of law and strategy, as well as the junction of war and peace because of their dual objectives. But with hybrid threats on the rise, some have begun to wonder if the mutual aid provisions established in the North Atlantic and EU treaties still apply in the context of the current security situation.

INTRODUCTION

Modern technologies have put humanity under new threats and risks. With the development of digital technologies, cyberattacks acquire complex, sophisticated forms, and cyberspace becomes increasingly vulnerable. Since cyberspace is not limited to geographical boundaries, one of the biggest challenges for mankind today is the fight against cybercrime. It is important to legalize cyberspace, to develop new norms of international law and new cyber doctrines. Following Pijpers et al (2020), defensive and offensive operations take effect in cyberspace itself. 2016 Warsaw Summit Communiqué, North Atlantic Treaty Organisation acknowledged the significance of cyberspace and positioned it among other domains including air, land, and sea (NATO, 2016). NATO is primarily focused on cyber defense, whereas individual Member States have started to take the initial steps toward developing offensive cyber capabilities. Cyberspace broadens and evens the playing field for States and non-State actors to influence individuals, groups, or other audiences, notwithstanding the many similarities between operations in all domains.

DOI: 10.4018/978-1-6684-8846-1.ch008

Emerging opportunities and dangers appear to unleash State power to alter public perception or reveal or delete material in cyberspace (Pijpers and Arnold, 2020).

The reduced obstacles to entry, anonymity, the unpredictability of the threat area, and lack of public transparency in cyberspace have given rise to threats like cyberwarfare, cybercrime, cyberterrorism, and cyber espionage from both strong and weak actors such as governments, organized crime groups, and even individuals (Yuchong and Qinghui, 2021). This renders cyber threats distinct from conventional security threats, which encompass government, cover a specific geographical area, and are transparent (Sarker, 2021). Therefore, before addressing the main topic of collective cyber defense, the question of what constitutes a cyberattack, what distinguishes it from other types of attacks, and whether or not virtually any attack that occurs in cyberspace can be regarded as an attack in the traditional and classic sense emerges. Hence, it is necessary to have an appropriate definition, for the introduction of the topic and its justification, and analysis.

FUNDAMENTAL CONCEPTS

Today information is everywhere. Communication, knowledge acquisition, intelligence gathering, and persuasion all include the use of information. In the end, it can be weaponized to sway a certain audience's perceptions and choices (Pijpers and Arnold, 2020).

Even though cyberspace is becoming more crucial for national security plans, the phrase has yet to be given a widely agreed definition. However, we can highlight a range of definitions provided by various actors, including Germany, the USA, the International Telecommunication Union (ITU), and the Tallinn Manual due to their major role and central position in information and communication technologies. Considering its significant role and strategic location within the EU, Germany provided the following definition of cyberspace as "…the virtual area of all information technology systems in the world which are or could be interconnected at data level" (Federal Ministry of the Interior, Building, and Community 2021, p.125).

According to the US National Institute of Standards and Technologies cyberspace stands for "the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (NIST 2012, p. B-3).

Moreover, the International Telecommunication Union (ITU) an agency of the United Nations, mentions the following elements, specifically the software that runs on computing devices, the transferred and stored data, as well as the information produced by these devices, are all included in the cyber environment. Such factors must be taken into account while discussing cybersecurity (ITU 2008).

The Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual) provides legal aspects of how international law applies to cyber disputes, as well as supports NATO with specialized multidisciplinary expertise in the areas of cyber defense research (Georgetown Law Library 2023). According to the manual, cyberspace is made up of both physical and immaterial elements, which alter, and exchange data across computer networks (Schmitt 2013).

Characteristics of Cyberspace

More specifically about cyberspace, Pijpers et al (2020) emphasize five factors that distinguish cyberspace from other domains, namely *reaching, time and speed, versatility and reusability, asymmetric effect, and*