Chapter 11
Conceptualizing Cyber-Security From EU Perspective

Ayse Kok
Bogazici University, Turkey

ABSTRACT

If the aim of the EU is the establishment of deeper cooperation with other nations within the context of cyber security in the future, platforms (e.g., the Task Force) should create an effective agenda that reflects the differences between the EU (soft power) and other countries such as China or Russia (hard power). Yet, there should not be any compromise in the principles and norms of these countries with regard to their Internet policies. Although this may sound too difficult to accomplish, it is not impossible given EU's increased emphasis on cybersecurity along with its evolving cybersecurity strategy.

INTRODUCTION

In 2004, ENISA (European Network and Information Security Agency) was founded in order to facilitate 'best' practice among Member States with regard to cyber security policies with regard to EU's Information Society agenda. In 2007, due to DDoS (Distributed Denial of Service) attacks on the public infrastructure of Estonia, the EU along with NATO and other related actors considered to change their approach. As a result, the EU's policy has been developed within the light of the Europe 2020 strategy. The European Cybersecurity Strategy (2013) and its Guidelines and Principles for Internet Resilience (March 2011) focus on the significance of global partnerships to address both military and civilian aspects of cyber security challenges.

According to EU Cybersecurity strategy, the Internet must be kept protected and 'open and free' based on the same values and principles that the EU considers for offline space (EU Cybersecurity Strategy). EU Cybersecurity Strategy and its Directive on Network and Information Security (NIS Directive) were published on 7 February 2013, to require the reporting of significant cyber incidents across all critical infrastructure sectors (NIS Directive 2013). For the first time, the EU tried to specify priorities with regard to the protection of cyberspace via means of this strategy as previously there was no coordination

DOI: 10.4018/978-1-7998-8954-0.ch011

with regard to the construction of an effective security ecosystem for cyberspace (Klimburg & Tirmaa-Klaar 2011).

This paper will be structured as follows: After a brief overview of the conceptual landscape of the EU's cyber security development, the suggested tools for cyber security policy of EU will be explained. Next an overview of the EU's way of dealing with cyber security threats will be explained. The final section will provide recommendations for EU's cooperation with other states on cybersecurity in the future.

Concepts and Approaches of the EU's Cybersecurity Policy

The existing body of academic literature with regard to the EU's action in cybersecurity is scarce as most of the available work focuses on the US and other regions (Kshetri, 2013), with no in-depth theoretical analysis of EU's cyber security policy. Various approaches such as managerial and strategic (Libicki 2007, 2009; Clarke & Knake 2010), historical (Carr 2009) and 'other approaches that focus on terrorists (Wiemann 2006; Colarik 2006) have been used. While the emphasis of such approaches has been more on recent cyber threats and how to establish the 'cyber peace' (Clarke & Knake 2010), other theoretically and methodologically driven works used innovative mixed-method (Deibert et al. 2012), regulatory (Brown & Marsden 2007) and other approaches that try to evaluate the extent of securitization of cyber policy (Dunn, 2007, 2008; Bendrath *et* al. 2007).

Cyber power has been so far one of the most frequently used concepts with regard to cyber security (Klimburg and Tirmaa- Klaar 2011; Betz and Stevens 2011; Klimburg 2011; Nye, 2010; Kramer et al. 2009). While Nye (2010) defines cyber power as the ability to utilize the digital pace to create an influence and gain advantages in other operational contexts (2010, p.4) he makes a distinction between information and physical instruments, as well as soft and hard power in cyber space, and provides examples of how they can be used both outside (extra cyberspace power) and inside (intra cyberspace power) (See Table 1).

Table 1. Instruments of power in cyberspace

	Intra Cyber Space	**Extra Cyber Space**
Information Instruments	Soft: Set standards & norms	Soft: Public campaign to influence opinion
	Hard: Denial of Service Attacks	Hard: Attack SCADA systems
Physical Instruments	Soft: Infrastructure to support activists of human rights	Soft: Protests to name and shame cyber providers
	Hard: Government controls over enterprises	Hard: Cut cables or bomb routers

(Source: Nye, 2010)

Other scholars such as Betz & Stevens (2011, p.44) acknowledge the fluidity of cyberspace and mention that and that various non-state and state actors, ranging from states to citizens, global networks and organizations, can have an influence at any point in time in order to exploit the possibilities offered by cyberspace. As a result, they conceptualize the cyber power in four distinct forms:

- **Compulsory***:* This occurs when one cyberspace actor makes use of direct coercion to change the behavior of another actor (hard power such as attacks on FBI systems);