


Chapter 17

Cyber–Attacks From the Political Economy Perspective and Turkey

Serpil Karlidag

 <https://orcid.org/0000-0002-6999-0570>

Giresun University, Turkey

Selda Bulut

 <https://orcid.org/0000-0003-1615-6897>

Ankara Haci Bayram Veli University, Turkey

ABSTRACT

Since cyber-attacks involve a wide range of actions, they are subject to various definitions and classification. As some of the attacks cover stealing data and information, some of them prevent the whole system from working. Some attacks are connected to political conflicts while others are caused by economic or social tensions. Due to the developments in new communication technologies, the espionage activities which were held by the governments previously have been also occurring in civil organizations. Espionage activities for political reasons as well as economic motivations can cause big damage. The fact that individuals and organizations do not take the necessary measures makes them easily the target of these attacks. While the problem is analyzing with a holistic approach, the need to examine the relations between institutions, social relations, information and hegemony from a moral point of view due to the concentration of constantly changing and developing technology on certain hands have precisely made this article necessary to deal with a critical economic political approach.

INTRODUCTION

Each field of modern life depends on computers and e-technologies. Together with rapid development of Information and Communication Technologies after 1990, and transfer of applications of both public and private sectors into electronic media have made each field of life be depended on IT. Such develop-

DOI: 10.4018/978-1-7998-3270-6.ch017

ments have brought forward cyber-security measures on the assumption that the cooperation between secret services, hackers and crime organisations has targeted state secrets and the information owned by private sector with relation to intellectual property rights (Başaran, 2017). As cybersecurity has started to be a vital concern for functioning of modern economy.

Cyber-attacks started to occur after 1990s have become a source of concern in terms of security and international relations, and the attention is started to be paid to the economic aspect of the case. As a matter of fact, cyberattacks have been determined in Global Risk Report of World Economic Forum as the third biggest global risk after bad weather conditions and natural disasters. The impact area of cyber-attacks, carried out for different purposes and by various techniques, expands covering many countries. As institutions and governments have been digitalised and their dependence on cyberspace increases day by day, they become targets of the attacks. Such situation carries the damage of cyberattacks beyond the individuals; it constitutes a major form of threat. Malicious activities, which are a kind of cybersecurity breach, are classified as cyberattacks and data breach. According to national intelligence directors, cyberattacks mainly change the data, and include physical impacts, such as deleting and impairment, which directly interfere in the activities. Data breach, on the other hand, does not interfere in ordinary course of business, instead it discloses the corporate data to third parties that do not have the authority to see or receive such data (White House, 2018). The attacks not only abuse trust of users in internet but also damage the activities of governments and accordingly affect the economic growth in a negative manner.

Gandhi et al. (2011) have put forward that cyberattacks result in psychological effects such as rapid dispersion of fear as a form of panic, beside the direct physical effects such as paralysation of certain systems like water, electricity, drainage, energy which are considered as critical infrastructures¹ and highly necessary in daily life, financial losses and prevention of access to information or disclosure of information in an unauthorised way.

Throughout the history, Access to information which is valuable for the power and market system has become extremely stunning together with networking. Due to information and communication Technologies, a broad data bank has been formed and accordingly cyberthreats targeting such data constantly increase and are used by sophisticated enemies. The threats can made by institutions as well as countries. Nation states mainly carry out such kind of attacks in order for industrial espionage; but they are also carried out for different purposes and motivations including political, economic, military and technical reasons. Such kind of attacks can also be made in order for ransom due to financial requirements or as retaliation to certain decisions or sanctions determined in the international level. The primary actors in this regard are considered as Russia, China, North Korea and Iran (White House, 2018). Technological resources, which cheapen continuously and are accessed easily, have facilitated the attacks. As hackers can easily Access to every kind of market, they can benefit from every kind of service and means and the ability for personalisation provided by the technology, cyberattacks reach the goals. The attacks are generally towards finance, health, trade secrets, intellectual property rights and reduction of reputation (Winward, 2016). Therefore, the actors carrying out the cyberattacks are not limited to the nation states mentioned above and rival institutions. The ones helping “hactivists” due to ideological grounds and propaganda, the ones selling personal data in dark web sites for ransoming or profit making, the opportunists using existing codes and techniques, unhappy or former workers seeking for revenge or gain constitute a large group too (White House, 2018). It is important for authorities to determine the material damage; however detection of the fact that hackers are especially interested in sensitive information and data plays a critical role in decreasing the risk of potential cyberattacks. As in all market failures,

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/cyber-attacks-from-the-political-economy-perspective-and-turkey/252751

Related Content

Unusual Features of the SARS-CoV-2 Genome Suggesting Sophisticated Laboratory Modification as a Biological Robot

Li-Meng Yan and Adrian David Cheok (2022). *Analyzing Current and Future Global Trends in Populism* (pp. 73-113).

www.irma-international.org/chapter/unusual-features-of-the-sars-cov-2-genome-suggesting-sophisticated-laboratory-modification-as-a-biological-robot/290101

Promoting the Representation of Historically Disadvantaged Students: What Educational Leaders Need to Know

Ibrahim M. Karkouti and Hazza Abu Rabia (2022). *Research Anthology on Racial Equity, Identity, and Privilege* (pp. 1155-1172).

www.irma-international.org/chapter/promoting-the-representation-of-historically-disadvantaged-students/296998

Zimbabwe Dancehall Music as a Site of Resistance

Blessing Makwambeni (2017). *Music as a Platform for Political Communication* (pp. 238-256).

www.irma-international.org/chapter/zimbabwe-dancehall-music-as-a-site-of-resistance/178016

Movement Control Order (MCO) - A Viable Legal Mechanism in the Management of COVID-19 Pandemic in Malaysia?

Suzana Muhamad Said, Aini Aman, Mohd Rohaizat Hassan and Omkar Dastane (2022). *Journal of Comparative Asian Development* (pp. 1-15).

www.irma-international.org/article/movement-control-order-mco---a-viable-legal-mechanism-in-the-management-of-covid-19-pandemic-in-malaysia/315650

China's Infrastructure Financing and the Role of Infrastructure in Awakening African Economies

Michael Mitchell Omoruyi Ehizuelen (2021). *Journal of Comparative Asian Development* (pp. 1-25).

www.irma-international.org/article/chinas-infrastructure-financing-and-the-role-of-infrastructure-in-awakening-african-economies/279131