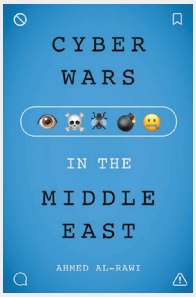
Cyberwars in the Middle East

By Ahmed al-Rawi
Rutgers University Press, 2021, 192 pages, $120, ISBN: 9781978810112

Reviewed by Flora Hajdarmataj, Anadolu University



Cyberwars can take place in many different contexts and are not limited to hacking: bots and trolls are also common elements of cyberwar today. In *Cyberwars in the Middle East,* Ahmed al-Rawi highlights some of these emerging digital phenomena in the Middle East. He discusses cyber conflict and cyberwar, including state-sponsored astroturfing, cyber armies, digital surveillance, spying tools, and the coordinated spamming and doxing operations often used to engage political opponents on social media. The author argues that hacking and other cyber operations are forms of online political disruption whose influence flows horizontally or vertically (top-bottom or bottom-up). Cyberoperations and politically motivated hacking are aggressive and militant forms of public communication used by tech-savvy individuals to affect politics and policies (p. 12). Using a form of vertical flow (top-bottom) online political disruption, nations such as the United Arab Emirates (UAE), Saudi Arabia, and Bahrain target their own citizens for their oppositional and activist political views by hacking and snooping on them. In contrast, hackers, who are often politically independent, practice bottom-up political disruption addressing issues related to the internal politics of their respective nations, as has been the case with Iraqi, Saudi, and Algerian hackers (p. 2). Another form of online political disruption is when hackers target ordinary citizens to express opposition to their political or ideological views.

National governments, terrorist organizations' hacking groups, and their affiliates constitute the hegemonic communication powers, employing hacking as a means of offense and defense against other nations and their citizens. As a part of the study of cyberwars in the Middle East, al-Rawi utilizes a model that examines the communications flows influencing our globalized world by using Kenneth Waltz's theory of structural realism in international relations and Manuel Castella's discussion of power and counterpower, in the sense that there are different types of communication flows that shape our networked society. This type of communication is considered a horizontal flow of online political disruption because these nation-states mostly use spy tools and surveillance inside their borders to target political activists and perceived opponents.

Cyberwars in the Middle East consists of six main chapters arranged geographically. The first chapter introduces a theoretical framework to situate hacking and other cyber operations. For instance, the Five Eyes intelligence alliance between the U.S., UK, Canada, Australia, and New Zealand has actively hacked and harvested data from many countries around the world. In Chapter 2, al-Rawi explains the international scope of cyber operations. As part of the international dimension of the online political disruption model, the U.S. and Russian cyber operations target and/

or involve the Middle East. For example, the U.S. Department of State's Digital Outreach Team initiative and other astroturfing online campaigns against terrorism fall within the category of vertical online political disruption (top-down) (p. 134). Al-Rawi concludes by stating that the U.S. astroturfing approach was ineffective because Arab audiences viewed it as miscalculated propaganda due to the general mistrust of U.S. intentions in the region. Using social media, the Russians utilized cyber operations via political trolls that were more advanced than U.S. cyber operations, especially in microtargeting Western versus Muslim Arab audiences.

The chapter 3 focuses on cyber operations and hacking as horizontal political disruptions because they often involve nation-states attempting to influence each other and international audiences vertically. Here, al-Rawi discusses cyber terrorism, which involves hacking into political systems to conduct cyberwars that complement offline terrorist activities: "Most authoritarian countries in the Middle East, for instance, automatically criminalize political hacking by classifying it as a form of cyberterrorism in order to silence political dissent and send a loud message to other would-be hackers that they cannot take this route in opposing the state and its legitimacy" (p. 26).

The chapter 4 addresses issues surrounding Islam and immigration while highlighting the differences between English and Arabic messages posted by Russian trolls. Russian trolls mostly associate Islam with liberals and the Black Lives Matter movement in English posts. This religion is negatively portrayed when far-right groups are microtargeted, yet Arabic-language messages are not antagonistic to Islam. So, it highlights techniques of othering through division and rage, with foreigners (especially Muslims and immigrants) frequently demeaned.

Chapter five focuses on regional rivalries and tensions in the Middle East North Africa (MENA) region, while chapter six discusses Arab cyber armies and the efforts of Arab hackers to disrupt online politics in their countries. In chapter 5, al-Rawi analyzes cybercorporations as horizontal forms of online political disruption. Based on a detailed analysis of the 2017 Qatari crisis, the author demonstrates that most Arab countries have either purchased or used offensive cyber measures and surveillance tools to hack their regional rivals and spy on political activists inside their territories. A few Arab countries, such as the UAE and Saudi Arabia, acquired more advanced spying tools and technology, though none of them can compete with Israel and, to a lesser extent, Iran.

In addition to an overview of a number of Arab hackers, an explanation of electronic attacks and cyber armies is given in the last chapter, which emphasizes the Syrian Electronic Army (SEA) (p. 106). Cyber armies are designed to disseminate pro-regime propaganda and attack political opponents, activists, and critics. Cyber armies often obtain limited Twitter account numbers by spamming, trolling, and reporting (squishing) coordinated and systematic actions. Cyberoperations like these are like war skirmishes happening continuously: "We find an active DIY Arab hacker culture where activists and hackers learn how to hack the government in order to expose corruption and nepotism" (p. 107). This aspect of cyber war is waged to create social justice and is theoretically part of the vertical (bottom-up) online political disruption model. Overall, hacking is a form of aggressive and militaristic public communication because hackers practice online political disruption and are some-

times sponsored, supported, or employed by states to achieve political goals.

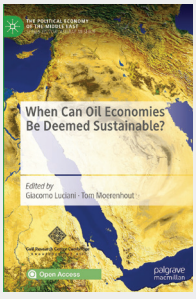
Cyberwars are likely to continue in various forms as spying technologies as regional rivalries become more intense. Online political disruption in the Middle East will not cease so long as political establishments remain unchanged. According to Valeriano and Maness (2015), cyberwar in the Middle East has the potential to escalate since it is closely linked to geopolitical developments in the region.

Cyberwars in the Middle East is a study that spans a decade of cybercorporations in the Middle East, presented as an investigation of several cases of cyberwars in international, regional, and internal politics. al-Rawi presents empirical findings based on several case studies using mixed methods; sources of the book include academic references, social media, newly declassified documents, the WikiLeaks archive, and news reports. Other scholars, experts, and practitioners will find al-Rawi's cyberwar model useful in studying other geographical regions and contexts. Al-Rawi encourages future research to examine the many unexplored aspects of this field, such as interviewing trolls to get a better understanding of their viewpoints and motivation.

When Can Oil Economies Be Deemed Sustainable?

Edited by Giacomo Luciani *and* Tom Moerenhout
Palgrave Macmillan, 2021, 365 pages, €39.99, ISBN: 9789811557286

Reviewed by Abdalrahman Migdad, İstanbul Sabahattin Zaim University



In answering the titular question, "when can oil economies be deemed sustainable?" the editors, who are also contributors, explore the economies of oil-dependent countries and the question of economic sustainability. Contributors to the book include economists and energy specialists in established research centers and agencies worldwide. *When Can Oil Economies Be Deemed Sustainable?* presents a real predicament connected to energy and sustainability: whereas energy is an immediate cause of pollution and environmental degradation, oil revenues are only sufficient to sustain oil economies in the medium term. So with no alternative to oil, oil economies will continue production and pollution will continue to rise.

The volatility of the energy market confirms the notion that oil revenues are not sustainable. Interruptions in supply and demand are the leading causes of such volatility, and the ongoing Russia-Ukraine war is the latest factor driving the price increase. Therefore, oil-dependent countries seek to establish trade diversification and the diversification of revenue sources. A sizable part of the book explores the economic threats with which oil resource countries must cope, a phenomenon known as the 'Dutch Disease.' The book also addresses sustainability and diversification in Gulf countries, as imbalances, wars, and crises, whether in the Gulf or similar regions, affect both suppliers and recipients of energy resources.