Chapter 11
Conflict in Cyberspace: The Case of the Middle East

Olivier Danino
French Institute for Strategic analysis (IFAS), France

ABSTRACT
States and non-states actors in the Middle East are totally aware about the strategic importance of cyberspace. They all use it in the conflicts where they are involved in order to improve, for example, their communication, propaganda or intelligence operations. Nevertheless, all these actors have different capabilities in the cyber field. This article sums up how Middle East governments are developing those offensive capabilities and how cyber has changed the way States handle the threat that they are facing. In the other hand, it analyzes how non-states actors are using cyber tools and what kind of targets they are reaching or they want to reach in the near future.

INTRODUCTION
The Middle East is one of the most contentious areas in the world. The issues are strategic, energy-related, religious and political. Territorial disputes are numerous. While the Israeli-Palestinian conflict may dominate the attention, it is not the only one. Iran and the United Arab Emirates, Yemen and Saudi Arabia, Syria and Israel, are examples of territorial disputes still unresolved. One of the major characteristics of the Middle East is the profusion of non-state actors. Some are relatively small. Others are more organized, like Hezbollah in south Lebanon and Hamas in the Palestinian territories. But states and non-state groups have a common point. They use every means at their disposal to defend their interests.

Cyber is especially useful for these objectives. Cyber is a tool for intelligence, sabotage and military operations, but it can also be used for communication and to develop an information and propaganda network. It can be used to launch different types of attacks which are inexpensive and difficult to trace. The actors of the region have different capabilities and different perceptions about the strategic importance of cyber. For some, the cyber domain is a national priority. For others, the focus is mostly to control the Internet and prevent cybercrime.

DOI: 10.4018/978-1-4666-8456-0.ch011
Conflict in Cyberspace

Usually, analysis of cyber issues in the Middle East is devoted to a specific event. The region is rarely studied in its entirety. The consequence is that the data available are scattered and fragmented, which makes synthesis difficult and demands an original approach. This study is therefore based on a variety of information, such as reports available online from university research centers, private and public international organizations, books on cyber, and analyses conducted by computer security firms about viruses detected during the last 5 years. This study is also based on interviews with French and foreign cyber experts, on conferences held in France and abroad, and on a corpus of documents available in French, English and Hebrew.

It must be emphasized that the cyber domain is still maturing. The definition of the word “cyber”, and its derivatives, varies according to experts and governments. Russians speak of “information technology” or “information terrorism”, where others evoke “cyber” or “cyberterrorism” (Adjemov et al., 2011). Moreover, two countries may use the same term in reference to different realities. The concept of cyberspace fluctuates from one country to another. For the U.S. Department of Defense (2012), cyberspace is “a global domain environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers”. In France, the National Agency of Information Systems Security (2011) defines cyberspace as “a communication space consisting of global interconnection equipment automated processing of digital data”.

Definition is not an easy matter, but for clarity we have to specify exactly what we understand by cyberspace. As Jean-Loup Samaan (2008) writes, “Security experts recognize three constituent layers of cyberspace: the physical layer, the syntactic stratum, and the semantic stratum. The physical layer consists of infrastructure, cables, routers and switches: it is the most concrete aspect of cyberspace. The syntactic layer links the other two strata formatting information in cyberspace, by giving it standards and protocols such as TCP / IP on which the Internet is based. Finally, the semantic stratum means the raw data transmitted by cyberspace and exploited by humans or machines. This information can range from simple email to the images transmitted by a reconnaissance UAV to its control station on the ground”.

An attack against cyberspace may therefore seek one of these three strata. It can be conducted by conventional means such as cyber. The aim of our study is to better understand how the different actors in the Middle East conceive cyberspace. We also examine the possible existence of partnerships between states and between state and non-state groups. In other words, we propose to understand how each actor discusses the cyber domain and the impact of cyber on the balance of forces in the Middle East.

1. CYBER STRATEGIES IN THE MIDDLE EAST

Each country has its own strategy on cyber issues but we can distinguish some common points and then four strategic blocks in the Middle East.

The first block is formed by Turkey alone. Turkey has shifted its global strategy from the goal of joining the European Union to the goal of strengthening certain alliances in the Arab world at the expense of its relationship with Israel. But in the field of cyber, Turkey turns toward organizations outside the Middle East like NATO and the UN. Its first two major participations in cyber exercises and simulation games were with those institutions. A cyber security drill was held in Istanbul on May 15th-16th 2014, in order to strengthen international cooperation and cyber defense. It was jointly organized by the International Telecommunication Union and the International Multilateral Partnership Against Cyber Threats (ITU-