



وزارة التعليم العالي والبحث العلمي

جامعة الموصل

كلية العلوم السياسية



التهديد السيبراني للأمن الإقليمي في القرن الحادي والعشرين:

إسرائيل أنموذجاً

رسالة تقدم بها الطالب

محمد أكرم محسن

إشراف

أ.م.د. مروان سالم علي

المُلخَص

ساهمت التحولات الاقتصادية والتكنولوجية المُتسارعة وغير المسبوقة في العقود الثلاث الأخيرة وفي ظل العولمة، من زيادة تشظي القوة وانتشارها بعيداً عن الدول إلى الفواعل الأخرى من غير الدول. فإلى جانب قوة الدولة الصلبة والناعمة ظهرت القوة السيبرانية والتي أصبح لها تأثيرها على المستويين المحلي والدولي، حيث أدت إلى تعدد مستويات القوة بين الفاعلين دون حصرها بالدولة، كما مكنت الفاعلين الأصغر في السياسة الدولية من ممارسة كل من القوة الصلبة والناعمة عبر الفضاء السيبراني (الإلكتروني)، وهو ما يعني تغييراً في علاقات القوى في السياسة الدولية. وأصبحت مسألة أمن الفضاء السيبراني مسألةً مُهمّةً على أجندة الأمن الدولي، خوفاً من تعرض المصالح الاستراتيجية ذات الطبيعة الإلكترونية إلى ساحة صراع دولي تُهدد الأمن الدولي.

ولإدراك "الإسرائيلي" المُبكر لأهمية القوة السبرانية والتفوق العسكري والعلمي، أُسرعت في استثمار ثروات طائلة في هذا المجال ساعيةً لأن تكون من ضمن الدول الخمس الرائدة عالمياً في مجال القوة السبرانية، وهذا ما جسد لها دافعاً مُتزايداً في تطوير منظومتها الإلكترونية حتى أصبحت اليوم من أوائل الدول التي أنتجت وطورت أحدث النظم الإلكترونية، التي لم يقتصر استخدامها لغرض حماية نظم الاتصالات ووسائلها؛ بل تعدت ذلك لاستخدام هذه التكنولوجيا والبرمجيات والفيروسات لأغراض عدائية وهجومية وأدخلتها في منظومتها العسكرية والحربية حتى أصبحت تُمارس دوراً عالمياً بين القوى الكبرى ولها ثقلها في هذه الأصعدة، فضلاً عن قيامها باستثمار جزء كبير من ميزانيتها ومجهودها الأمني، لإقامة مفهوم الدفاع الإلكتروني، وعدّ قرار إنشاء هيئة السايبر "الإسرائيلية"، تقدماً ملحوظاً في أسلوب معالجة الحكومة لمسألة التهديد السيبراني، لتُجسد "إسرائيل" بذلك تهديداً للأمن الدولي.

تم تقسيم الرسالة، فضلاً عن المُقدمة والخاتمة والاستنتاجات إلى ثلاثة فصول رئيسة، عرض الباحث في الفصل الأول إطاراً مفاهيمياً نظرياً عن التهديد السيبراني للأمن الدولي. أما الفصل الثاني فبين التهديدات السيبرانية (الإلكترونية) المؤثرة في الأمن الدولي. ودرس الفصل الثالث التهديد السيبراني "الإسرائيلي" للأمن الدولي.

2022 A.D.

1444 A.H.



**Ministry of Higher Education and
Scientific Research**

Mosul University

College of Political Sciences



**The Cyber Threat for Regional Security in the Twenty–
First Century: Israel as a Model**

By

Mohamad Akram Muhsen

Supervised By

Assit Prof.Dr. Marwan Salim Ali

Abstract

During the last three decades of globalization, the rapid and unprecedented economic and technological transformations have contributed to the further fragmentation and spread of power away from states to other non-state actors. In addition to the solid and soft power of the State, cyber power has emerged and has had an impact at the domestic and international levels, leading to multiple levels of power among actors without limiting it to the State and enabling more minor actors in international politics to exercise both solid and soft power through cyberspace. This power resulted in a change in power relations in international politics. Cybersecurity has become an essential issue on the international security agenda, fearing that strategic interests of an electronic nature will be exposed to an international conflict threatening international security.

Because of Israel's early realization of the importance of cyber power, military, and scientific superiority, it has accelerated to invest considerable wealth in this area, seeking to be among the five world leaders in cyber power. Israel demonstrated an increasing motivation in the development of its electronic system to become one of the first countries to produce and develop the latest electronic systems, which have not only been used to protect communication systems and their means. It has utilized it in its military system to become a global role among the major powers and has its weight at these levels. Moreover, Israel invested a large part of its budget and security effort to establish the concept of electronic defense, and the decision to establish the Israeli Cyber Authority has promised significant progress in the government's handling of the issue of cyber threat, thus reflecting Israel as a threat to international security.

The study focuses on a fundamental problem: the global techno-information variables that have emerged in the twenty-first century have become a clear threat to international security because of the increasing spread of cyberattacks in cyberspace. The study is based on the premise that, in the twenty-first century, the international security system faces a range of strategic threats. Cyber threats are at the forefront of those threats as the world order (international and non-international) seeks to employ cyber power in their international interactions. Therefore the more effective the use of cyber power by these actors in their interactions, the more negatively affects and threatens international security and then the emergence of new patterns of international conflicts in the general inability of states to encounter cyber threats, thus transforming these conflicts from mere maneuvers into real-life wars with the main field of digital space and the militarization of cyberspace.

Based on the study's problem and hypothesis, the study is divided into three main chapters: introduction, results, and conclusions. In the first chapter, the researcher presents a theoretical, conceptual framework on the cyber threat to international security. The second chapter is entitled Cyber Threats affecting international security. Chapter three is titled The Israeli Cyber Threat to International Security.