

Ministry of Higher Education and Scientific Research  
University of Salah Bounider –Constantine 3-



Faculty of Political Sciences  
International Relations Department

Serial N°: .....

Code: .....

International Relations Field

Specialty of Security and strategic studies

Thesis submitted in partial fulfillment of the requirements for the  
Master Degree

**Cyber warfare as a tool in International Relations:  
the case of the USA in Syria**

**Submitted by:**

*Benkherouf Ahlem*

**Supervised by:**

*Mr. Ikhlef Abdecelem*

**Board of Examiners:**

<i>Dr. Frimeche Malika</i>	<i>University Constantine 3</i>	<i>Chairwoman</i>
<i>Mr. Ikhlef Abdecelem</i>	<i>University Constantine 3</i>	<i>Supervisor</i>
<i>Dr. Menaifi Ferial</i>	<i>University Constantine 3</i>	<i>Examiner</i>

**Academic year: 2019/2020**

# *List of contents*

## **List of Contents:**

<b><i>Dedication.....</i></b>	<b><i>i</i></b>
<b><i>Acknowledgments.....</i></b>	<b><i>ii</i></b>
<b><i>Research plan:.....</i></b>	<b><i>iii</i></b>
<b><i>Introduction:.....</i></b>	<b><i>1</i></b>
<b><i>Chapter one: Cyber warfare: A conceptual and theoretical framework:.....</i></b>	<b><i>6</i></b>
<b><i>1 Concept of cyber warfare:.....</i></b>	<b><i>8</i></b>
1.1 Definition of Cyber warfare:.....	8
1.2 History of cyber warfare:.....	14
1.3 Related concepts of Cyber warfare:.....	21
<b><i>2. Strategic Cyber warfare:.....</i></b>	<b><i>32</i></b>
2.1 Purpose of Cyber warfare:.....	32
2.2 Plausibility and Limits of Cyberwar:.....	34
2.3 Weapons and warriors of Cyber Warfare:.....	37
<b><i>3. Cyber Warfare and International relations theories:.....</i></b>	<b><i>39</i></b>
3.1 Neorealism and Cyber Warfare:.....	39
3.2 Liberalism and Cyber Warfare:.....	41
3.3 Constructivism and Cyber Warfare:.....	43
<b><i>Chapter two: Impact of Cyber warfare's types on International Relations:.....</i></b>	<b><i>48</i></b>
<b><i>1. Stat actors in cyber warfare.....</i></b>	<b><i>50</i></b>
1.1 Cyber superpowers.....	50
1.2 Cyber Warfare: The Threat from Nation States:.....	56
<b><i>2. Non-stat actors in cyber warfare:.....</i></b>	<b><i>59</i></b>
2.1 Hacktivists:.....	59
2.2 Cyber terrorists:.....	62
2.3 Organized cybercriminals:.....	65
<b><i>3. International solutions for cyber warfare:.....</i></b>	<b><i>67</i></b>
3.1 Cyber Alliances:.....	67
3.2 International law and cyber warfare:.....	69
<b><i>Chapter three: American Cyber Warfare in Syria: Operations and Results.....</i></b>	<b><i>73</i></b>
<b><i>1. Syrian Civil Conflict in the Cyber Environment:.....</i></b>	<b><i>75</i></b>
1.1 Syrian cyber strategy and its victims.....	75

**Abstract:** Because of the increasing reliance of developed countries on internet networks in the 21st century, cyberspace has emerged as a new dimension and another challenge for nations, as they no longer anticipate attacks that may occur on their land, air and sea territory. They are preparing for a new type of warfare, namely cyber warfare, which is the cyberspace that takes the Internet and computers as its field. This type of warfare has endangered State security, thus requiring the reformulation of security in line with the new developments in cyberspace in international relations. And it is become a tool in international relations, this new revolutionary element of cyber warfare has moved the international arena of interactions to a new kind of power race of global cyberspace control to ensure that all the nations secure their strength and prestige. This rivalry or race has changed the structure of the international system with the emergence and rise of new electronic powers: Israel, China, and Russia.... Competing USA who has undermined its international standing as a dominant superpower in the international community.

**Keywords :** Cyber warfare, cyberspace, USA cyber strategy, cyber-attacks, cyber terrorisme.

### المخلص:

وبسبب الاعتماد المتزايد للبلدان المتقدمة على شبكات الإنترنت في القرن الحادي والعشرين، برز الفضاء الإلكتروني كبعد جديد وتحدي آخر للدول، حيث أنها لم تعد تتوقع الهجمات التي قد تحدث على أراضيها البرية والجوية والبحرية. إنهم يستعدون لنوع جديد من الحرب، وهو الحرب السيبرانية، الفضاء السيبراني الذي يتخذ الإنترنت وأجهزة الكمبيوتر كمجال لها. وقد عرّض هذا النوع من الحروب أمن الدولة للخطر، مما يتطلب إعادة صياغة الأمن بما يتماشى مع التطورات الجديدة في الفضاء السيبراني في العلاقات الدولية. هذا العنصر الثوري الجديد للحرب السيبرانية قد نقل الساحة الدولية للتفاعلات إلى نوع جديد من سباق القوة للسيطرة على الفضاء السيبراني العالمي لضمان أن جميع الدول تؤمن قوتها وهيبتها. وقد غير هذا التنافس أو العرق بنية النظام الدولي مع ظهور وصعود قوى إلكترونية جديدة: إسرائيل والصين وروسيا... المتنافسة مع الولايات المتحدة الأمريكية التي قوضت مكانتها الدولية كقوة عظمى مهيمنة في المجتمع الدولي.

**الكلمات المفتاحية:** حرب سيبرانية، فضاء سيبراني، الاستراتيجية الأمريكية السيبرانية، الهجمات السيبرانية، الارهاب السيبراني.

## *List of contents*

1.2	Iran’s and Russia’s influence on the Syrian strategy .....	78
<b>2.</b>	<b>American cyber strategy: .....</b>	<b>81</b>
2.1	Preception of Cyberwarfare in the US Government: .....	81
2.2	US cyber tools and organizations: .....	84
<b>3.</b>	<b>U.S Cyber-attacks:.....</b>	<b>86</b>
3.1	US against Syrian government: .....	86
3.2	US cyberwar against ISIS:.....	87
<b><i>Conclusion:.....</i></b>		<b><i>91</i></b>
<b><i>Bibliography: .....</i></b>		<b><i>94</i></b>
<b><i>List of Contents:.....</i></b>		<b><i>104</i></b>