

# تحولات مفهوم القوة في الفضاء الإلكتروني

## مقاربة سياسية

بلقاسمي مولود

باحث دكتوراه في الدراسات الدولية  
المدرسة الوطنية العليا للعلوم السياسية  
بن عكنون-الجزائر.

حادي إبراهيم

باحث دكتوراه في الدراسات الأفريقية  
كلية العلوم السياسية و العلاقات الدولية  
جامعة الجزائر 03

### ملخص:

تحاول هذه الدراسة تسلیط الضوء على تحولات مفهوم القوة في الفضاء الإلكتروني، من خلال تأثير التكنولوجيا الرقمية على استخدامات مفهوم القوة في الصراعات الدولية وخاصة في مجال الحروب، فكثير من الدول تسعى للدخول لمجال الفضاء الإلكتروني كساحة للصراعات الدولية، وكمجال للحروب عن طريق استخدام القوة والقدرات التكنولوجية.

فمفهوم القوة تأثر بالטכנولوجيا الرقمية، وإنقلت الدول من مستوى الحروب والتهديدات الأمنية التقليدية إلى مستوى حروب وتهديدات من نوع مختلف، وبوسائل وأساليب مختلفة، فالصراع الإلكتروني أحد أوجه الصراع الذي يهدد الأمن الدولي، حيث يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة ويتسبب في شلل البنية المعلوماتية والاتصالية للطرف المستهدف عن طريق أسلحة وقدرات تكنولوجية وعسكرية كبرامج التجسس والفيروسات.

### Abstract :

This study is trying to treatment shifts the concept of power in cyberspace, Through the influence of digital technology on the uses of the concept of force in international conflicts and

wars, especially in the field, Many countries are seeking to enter the field of cyberspace Square to international conflicts, and as an area of wars through the use of force and technological capabilities.

The concept of power influenced by digital technology, They moved states of the level of war-traditional security threats to the level of wars and threats of a different kind, and Means of different methods, E-conflict aspects of a conflict that threatens international security, Where one of the parties to the conflict can be signed and caused heavy losses in the Shell IT and communication infrastructure through weapons and military and technological capabilities as a platform for spyware and viruses.

#### مقدمة:

يعد ظهور ثورة تكنولوجيا المعلومات نقطة تحول كبيرة في جميع المستويات وخاصة في مجال الحروب،أو في إدارة الصراعات المسلحة، وخلال العشرين عاماً المنصرمة ،حدث نمو ضخم في عدد خدمات الحاسوب والشبكات، وفي نفس الوقت، يزداد عدد الأفراد الذين يسعون نحو استغلال قابلية الإصابة في الأجهزة المتصلة بالشبكات وأنظمة وتطبيقات الحاسوب.

وبهذا فقد دخل المجال الإلكتروني على مایيد و ميادين الحرب بصفة خاصة ومجال العلاقات الدولية بصفة عامة، حيث من المتوقع أن تكون الحروب الإلكترونية cyberwar السمة الغالبة إن لم تكن الرئيسية للحروب المستقبلية في القرن الواحد والعشرين.

#### الإشكالية:

ومن هذا المنطلق نطرح الإشكالية التالية:  
مامدى تحول مفهوم القوة في الفضاء الإلكتروني في القرن الواحد والعشرين؟

## المحور الأول: مفهوم القوة في العلاقات الدولية.

إن مفهوم القوة من المفاهيم الأساسية في الفكر السياسي، ترجمتها للغة الإنجليزية **POWER** وللغة الفرنسية **POUVOIR**. فهي في تعريفها اللغوي القدرة على التأثير في الآخرين وهي مفهوم أساسى في العلاقات الدولية.<sup>١</sup>

مفهوم القوة يعد مفهوما شائعا لـ الاستعمال ويحمل معانى مختلفة فالقوة التي يمتلكها شخص أو هيئة أو دولة تحدد مركزه وموقعه وقدرتها على التأثير على المحيط الذي ينتمي إليه، ويمكن إجمال مفهوم القوة في ثلاثة مفاهيم:

1. إمتلاك قوة يعني إمتلاك شيء واستعماله لأهداف معينة ومختلفة.
2. عامل متحرك، فحسب المدرسة الواقعية فإن الصراع من أجل القوة هو الدافع لسلوكيات الدول إتجاه بعضها البعض.
3. القوة سمة أو خاصية تطبع علاقة الأطراف بعضها بالبعض الآخر، بسبب الفارق في القوة بين الإثنين.

### أولاً: القوة الصلبة.

تعتبر القوة الصلبة أكثر أنواع القوة التي سيطرت لفترة طويلة في مجال العلاقات الدولية، حيث إستخدمت الدول للقوة الصلبة من أجل تحقيق مصالحها، وتكون من عناصر القوة المادية، والمتمثلة في القوة السياسية والعسكرية والاقتصادية، وقد ارتبطت القوة الصلبة بـ المدرسة الواقعية، وقد عرفها جوزيف ناي تعرضا شاملا، حيث يرى أنها تعني: "القدرة على استخدام الجرعة عن طريق الأدوات الاقتصادية، بهدف التأثير في سلوك الآخرين".

كما تتعدد صور وأشكال استخدام القوة الصلبة في الساحة الدولية، وهنا يمكن التمييز بين خمسة أنماط لاستخداماتها تمثل في:

- ✓ نمط الإكراه.
- ✓ نمط التخريب.
- ✓ نمط الردع.
- ✓ نمط الدفاع.

✓ نمط التدخل العسكري المباشر.<sup>2</sup>

ثانياً: القوة الناعمة.

قد طرح مفهوم القوة الناعمة لأول مرة بشكل أكاديمي سنة 1995 م من طرف البروفسور الأمريكي جوزيف ناي من خلال كتابه الطبيعة المتغيرة للقوة الأمريكية، حيث يرى ناي أن القوة الناعمة تستخدم لتبين مستويات التأثير الكبير للثقافة والقيم والأفكار على سلوك الآخرين، مقارنة بالإجراءات والوسائل القسرية، انتلاقاً من استخدام القوة الصلبة، وقد إحتلت القوة الناعمة مكانة كبيرة على المستوى الدولي بعد الحرب الباردة، تحديداً بعد أن تبين من خلال القضية العراقية والأفغانية، أن القوة العسكرية والعقوبات لم تجد نفعاً، كما تشير الحالة الإيرانية إلى نفس النقطة.<sup>3</sup>

ثالثاً: القوة الذكية.

القوة الذكية هي مزيج بين القوة الصلبة والقوة الناعمة، وقد أشار جوزيف ناي إلى مفهوم القوة الذكية على أنها: "القدرة على الجمع بين القوة الصلبة والقوة الناعمة، في إستراتيجية واحدة، للتأثير في الآخرين"، كما أن القوة الذكية تقوم على الحد من الإستخدام المفرط للأدوات العسكرية في مواجهة الأزمات وهذا موازاتها مع تطور عصر المعلومات والتكنولوجيا الرقمية مع الإحتفاظ بالقوة الصلبة، وتعتمد القوة الذكية كاستراتيجية على خمسة عناصر تمثل في:

- ✓ تحديد الأهداف والنتائج المرجوة.
- ✓ معرفة الموارد المتاحة.
- ✓ معرفة الأهداف والأولويات المراد التأثير فيها.
- ✓ أي نوع من القوة سيتم الاعتماد عليه.
- ✓ تقدير احتمالية النجاح.<sup>4</sup>

وفي هذا السياق يجب علينا التفرقة بين القوة الكامنة والقوة الفعلية والحقيقة أو المستخدمة والتي تنتج عن عملية تحويل للقوة الأولى والتي تكون لها ضوابطها التنظيمية والتقريبية والوصفية والتي تقدر مدى نجاحها.<sup>5</sup>

وبهذا فإن مفهوم القوة الذي يهمنا في هذا المقال هو أن القوة نسبية وهي القدرة على التأثير في سلوكيات الآخرين وفي البيئة والمحيط، ووفق تصور ومنظور أن القوة لها منهج قياس، وهي مجموعة المقومات التي تشكل درجة قوة الدولة، فإن وصف دولة في سياق تلك النقطة بأنها قوية، لا يعني أنها قادرة على التأثير في سلوك الآخرين في كل المجالات، وبشأن كل القضايا، كما أن حيازة دولة ما لعنصر قوة محدد لا يعني أنها قادرة على استخدامه للتأثير على كل أنماط السلوك المحيطة بها.

## المحور الثاني: مفهوم التكنولوجيا الرقمية والفضاء الإلكتروني.

### أولاً: التكنولوجيا الرقمية.

ترتكز التكنولوجيا الرقمية على اختزال المعلومات بشيء محدد كالنصوص أو الصورة أو الصور ومن السهولة بمكان المحافظة على المعلومات في صورتها الأصلية، ويرجع ذلك إلى أن المعلومات الرقمية تتكون من الصفر والواحد، حيث إن التكنولوجيا الرقمية تجعل المعلومات أكثر سهولة ودقة عند معالجتها بالكمبيوتر مما يؤدي إلى إنتاج أعمال ومؤثرات صوتية أو صوئية أكثر تطوراً، وقد أثرت التقنية الرقمية على الحياة وتطورها، وانعكس ذلك في الأجهزة والأدوات من التلفونات الرقمية والستاليت الرقمي والمصانع والاتصالات حتى الأجهزة المنزلية مثل الغسالات والتلفزيونات، ونسبة لكثرة الأجهزة التي تستخدم التقنية التماضية فإن هناك أدوات تعمل على تحويل المعلومات الرقمية إلى تماضية حتى تكون صالحة للعمل مع الخطوط التليفونية بجانب تحويل المعلومات الرقمية الآتية من خطوط التليفون إلى معلومات رقمية تعامل مع الكمبيوتر.

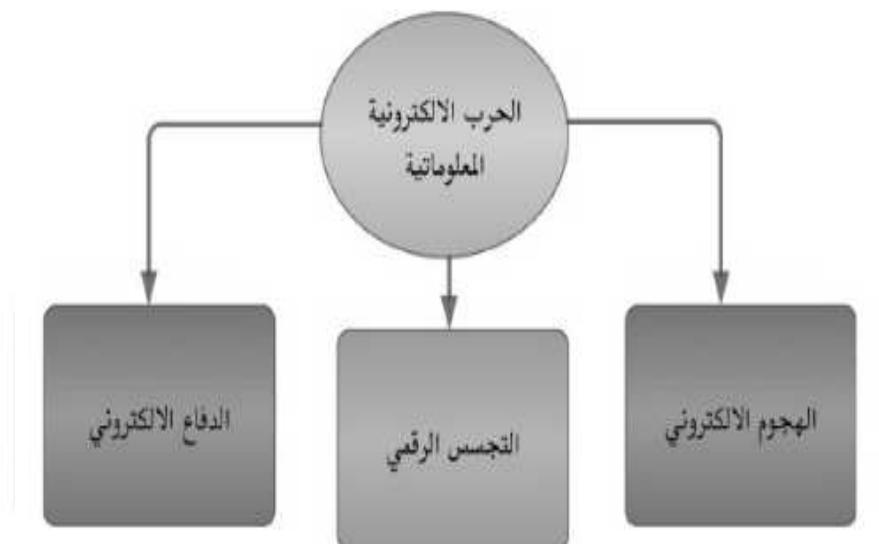
### ثانياً: الفضاء الإلكتروني.

تستخدم كلمة Cyber مقتربة بكلمة Space لتعبر عن أشهر تعبير في عصر المعلومات واستخدمت Cyberspace للتعبير عن الأنترنت في عام 1991، وأصبح هذا المفهوم أشمل وأوسع من الانترنت ليضم كل الاتصالات والشبكات وقواعد البيانات ومصادر المعلومات، وأصبحت بنية النظام الإلكتروني تعني المكان الذي لا يعده جزءاً من العالم المادي أو الطبيعي حيث أنه ذو طبيعة رقمية إفتراضية إلكترونية حيوية تعمل من خلال

خطوط الهاتف وكابلات الاتصالات والألياف البصرية وال WAVES الكهرومغناطيسية، ووصف "William Gibson" العالم الإلكتروني بأنه: "عبارة عن شبكات الكمبيوتر الخيالية تحتوي على كم هائل من المعلومات التي يمكن الحصول عليها لتحقيق الثروة والسلطة".<sup>6</sup>

وتعريف "الاتحاد الدولي للاتصالات" لفضاء الإلكتروني بأنه: "المجال المادي وغير المادي الذي يتكون أو ينبع من عناصر هي: أجهزة الكمبيوتر، والشبكات والبرمجيات وحوسبة المعلومات، والمحتوى ومعطيات النقل والتحكم، ومستخدمو كل هذه العناصر"، حيث تعد هذه العناصر العامل المشترك في جميع محاور استخدام الفضاء الإلكتروني، سواء كانت الجهات قادرة على تعظيم قيمتها وقدراتها بما فيها رفع كفاءة العنصر البشري أم كانت في مرحلة متأخرة.<sup>7</sup>

وبهذا فإن التعريفات نسبية تتوقف على طبيعة كل دولة أو كيان، وعلى مدى وقدرته على تحديد رؤيته واستراتيجيته للتعامل مع مجال الفضاء السيبراني بشقيه العسكري والمدني، وقدرته على إستغلال المزايا ومواجهة المخاطر الكامنة في هذا المجال، ومثال ذلك هناك من عرف الفضاء الإلكتروني بوصفه الدرع الرابع للجيوش الحديثة إلى جوار القوات الجوية والبحرية، وخاصة أن عصر الإنترنت شهد بداية الحديث عن المعارك حقيقة تدور في هذا العالم الافتراضي، وهناك من يرى أنه يمثل البعد الخامس للحرب.<sup>8</sup> وبهذا فإن الحرب الإلكترونية المعلوماتية تتكون من هجوم إلكتروني وتجسس رقمي ودفاع إلكتروني.<sup>9</sup>



شكل يوضح أشكال الحرب الإلكترونية المعلوماتية

المصدر: عباس بدران، "الحرب الإلكترونية الاشتباك في عالم المعلومات"، بيروت: مركز دراسات الحكومة الإلكترونية، 2010.

### المحور الثالث: أثر التكنولوجيا الرقمية على مفهوم القوة.

إن للتكنولوجيا الرقمية أثر هام على تطور ممارسة القوة والنفوذ في العلاقات الدولية، ذلك لما للمعلومة من أثر هام في حسم الصراعات الدولية، ويصبح من الضروري الوقوف على الفواعل والأطراف التي تمارس هذه القوة سواء كانت فواعل من الدول أو من غير الدول، وفي هذه الحالة يصبح مجال ممارسة القوة هو الفضاء الإلكتروني، وأطرافه هي الدول والفواعل من غير الدول وأدواته برامج حاسوب وవירוסات إلكترونية عوضا عن الأسلحة التقليدية لإختلافات عديدة كما يظهر في هذا الجدول.<sup>10</sup>

كما أن الفرق بين السلاح الرقمي والسلاح التقليدي واضح من خلال الجدول الذي يبين الفوارق في حجم الخسائر والتأثير.<sup>11</sup>

السلاح التقليدي	السلاح الرقمي	
عالية جداً	محدودة	<b>خسارة الأرواح</b>
يعتمد على نوعية السلاح - محدود يقاس بالكيلومترات	طالع آية نقطلة وصلت إليها الانترنت - حتى الفضاء	<b>المدى بالكيلومتر</b>
متقطعة	عالية	<b>التاثير بالرأي العام</b>
عالية	عالية	<b>الحرب النفسية</b>
عالية	متقطعة	<b>كلفة الاقتناء والصيانة</b>
متقطعة	عالية	<b>الاستخدام للتجسس</b>
مرة واحدة - إطلاق ثم تججير	مرات عديدة - ملائماً بطيء السلاح الرقمي تحت سيطرة القيادة	<b>عدد مرات الاستخدام</b>
مهارات خشنة	مهارات ناعمة	<b>المهارات البشرية المطلوبة</b>

### جدول يوضح الفرق بين السلاح الرقمي والسلاح التقليدي

المصدر: عباس بدران، "الحرب الالكترونية الاشتباك في عالم المعلومات"، بيروت: مركز دراسات الحكومة الالكترونية، 2010.

فبفضل ثورة المعلومات ومع ظهور الإنترت وموقع الويب Web اصبح الفضاء الإلكتروني أحد العناصر الرئيسية التي تؤثر في النظام الدولي بما يحمله من أدوات تكنولوجية تلعب دوراً مهماً في عملية التعبئة والحشد في العالم فضلاً عن التأثير في القيم السياسية وأشكال القوة المختلفة سواء كانت صلبة أو ناعمة.

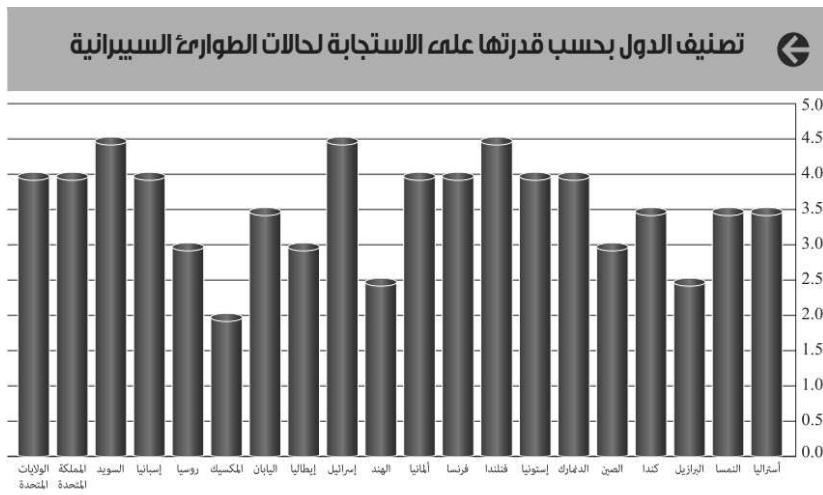
أصبحت القوة الإلكترونية حقيقة أساسية في العالم بكل مظاهرها المتنوعة بما تقدمه من دعم ومساندة في العمليات الحربية وال المجالين الاقتصادي والسياسي، بالإضافة إلى ثورة المعلومات والمعرفة والتي يكمن دورها في بروز مجتمع المعلومات الدولي والاقتصاد الإلكتروني الذي أثر على طبيعة النظام الدولي في مل يتعلّق بالتقسيم الدولي للعمل، كما يؤثّر على أنماط التفاعلات بين القوى الاقتصادية الدولية والتأثير على القوة السياسية بالتأثير على عمليات صنع القرار في النظام الدولي.<sup>12</sup>

وبهذا فإن تأثير التكنولوجيا الحديثة على مفهوم القوة يظهر من خلال رفع مستوى الحرب من حروب تقليدية سواء برية أو بحرية أو جوية إلى حروب إلكترونية بأبعاد ومستويات جديدة، مع قدرة هذه الهجمات والحروب الإلكترونية على التدمير وإلحاق الضرر بإستخدام أسلحة رقمية يصعب تعقيبها والدفاع والحماية منها.

**المحور الرابع: علاقة القوة والأمن الدولي بالفضاء الإلكتروني.**

تستخدم الدول الفضاء الإلكتروني لإعتبارات الأمان والقوة وتعظيم معرفتها وسباقها العلمي والبحثي، والقدرة أيضاً على تحقيق السلم والأمن والتفاهم الدولي من خلال دور الفضاء الإلكتروني كأداة إتصال ووسيلة إعلام دولية.

وهناك علاقة مابين الفضاء الإلكتروني والأمن الدولي تتضح في حيث يوجد المحتوى المعلوماتي العسكري والأمني والفكري والسياسي والإجتماعي والإقتصادي والخدمي والعلمي والبحثي في الفضاء الإلكتروني، خاصة مع توسع نموذج الحكومات الإلكترونية من جانب العديد من الدول وإتساع نطاق مستخدمي وسائل الإتصال وتكنولوجيا المعلومات في العالم، حيث أصبحت قواعد البيانات القومية في حالة إنكشاف خارجي، وهذا ما يعرضها لخطر هجمات وقرصنة إضافة إلى الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريض ودعم للمعارضة الداخلية للنظام الحاكم، مما استدعي تطوير كثير من الدول لقدراتها على الاستجابة لحالات الطوارئ السيبرانية كما يوضح هذا الشكل.<sup>13</sup>



شكل يوضح تصنيف الدول حسب قدراتها في الفضاء الإلكتروني.

المصدر: ربيع محمد يحيى، ”إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط“، مجلة رؤى إستراتيجية، 2013.

إن الصراع الإلكتروني أحد أوجه الصراع الدولي، حيث يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة بالطرف الآخر وأن يتسبب في شلل البنية المعلوماتية والاتصالية الخاصة به وهو ما يسبب خسائر عسكرية وإقتصادية من خلال قطع أنظمة الإتصال بين الوحدات العسكرية أو سرقة معلومات سرية عنها أو التلاعب بالأجهزة والحواسيب، وبالرغم من فداحة الخسائر فإن الأسلحة بسيطة لا تتعذر الكيلوبايت تمثل في فيروسات إلكترونية تخرب شبكة الحاسوب الآلي وتنشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية وهي بذلك لاتفرق بين المقاتل والمدني وبين العام والخاص وبين السري والمعلوم.<sup>14</sup>

وبهذا فإن الحروب الإلكترونية هي المستوى الأخطر من الصراع والنزع والذراع والتي تعتبر مصدر من مصادر التهديد وخاصة وأن الجماعات الإرهابية والإجرامية في تزايد مستمر وتسعي لإستخدام هذا المجال لتهديد الأمن الدولي، وتشير تقارير أنه من المتوقع أن تصبح الحروب الإلكترونية نموذجاً تسعى إليه العديد من الجهات، وذلك بسبب تزايد عدد الهجمات الإلكترونية.<sup>15</sup>

تعتبر الحرب الإلكترونية المستوى الأخطر من النزع في المجال الإلكتروني، وتعتبر جزءاً من الحرب المعلوماتية في مفهومها الواسع، وتهدف إلى التأثير في الإرادة السياسية للمستفيد وعلى قدرته في صنع القرار، وكذلك من أجل التأثير في مواجهات القيادة العسكرية.<sup>16</sup>

#### المحور الخامس: نماذج لصراعات وحروب إلكترونية.

يستطيع بعض الجماعات والأفراد أن تقوم بأعمال قرصنة إلكترونية أو تجسس أو إرهاب إلكتروني، لكن على مستوى الحروب الإلكترونية فالامر متعلق ببناء جيوش إلكترونية كاملة بقدرات هائلة وموارد ضخمة واستهداف لموقع وبني إستراتيجية، وهذا لا يتيح إلا للدول قادرة على الاستثمار في هذا المجال.

وإدراكاً منها لهذا الواقع، تنشط كثير من الدول في هذا المجال لاسيما الولايات المتحدة الأمريكية وروسيا والصين وإنجلترا وفرنسا وإسرائيل، وبعض الدول من الصنف الثاني

والثالث كالهند وباكستان وكوريا الشمالية وإيران وذلك بصورة صامته من أجل بناء قدراتها في هذا المجال، وذلك من خلال أعمال دفاعية وهجومية في الفضاء الإلكتروني.<sup>17</sup>

#### أولاً: الاستعدادات الهجومية.

تعتبر الصين وروسيا من أكبر الدول لتطوير إستعداداتها الهجومية في المجال الإلكتروني، إذ تعتبر الصين من أكبر الدول المطورة لإستعداداتها الهجومية، وهي فعلاً من الدول التي تدمج مفهوم القوة التكنولوجية في عقيدتها العسكرية وتؤكد الورقة البيضاء للأمن القومي لسنة 2006 على أن الهدف الرئيسي لبناء جيش قوي وحديث هو فوزه في مجال الحروب المعلوماتية، ولأن الصين ليست بالمستوى العسكري للولايات المتحدة الأمريكية والروسية فهي تحاول أن تستغل البعد الإلكتروني لتطوير قدراتها الردعية في هذا المجال.

أما روسيا فهي تسعى لتطوير قدراتها في الحرب الإلكترونية لاسيما في الشق الهجومي، فقد أتتت بالوقوف وراء العديد من الهجمات الإلكترونية مع عدم وجود دليل مادي على ذلك، لكن الواضح أن روسيا بعد إنهايار الإتحاد السوفيتي تعتمد على وسائل أقل تكلفة وأكثر فاعلية في مواجهة الولايات المتحدة الأمريكية وحلف شمال الأطلسي، إذ يعتبر الفضاء السيبراني أهم مجال للمواجهة في ظل التفوق العسكري الأمريكي والناتو.<sup>18</sup>

#### ثانياً: الاستعدادات الدفاعية.

تعتبر الدول المعتمدة على الأنترنت والشبكات المعلوماتية الأكثر عرضة للنتائج الكارثية لأي حرب إلكترونية تشن على مستوى عالي ودقيق، ولأن الأفضلية في هذه الحروب للهاجم عادة وليس للمتحصن، تسعى العديد من الدول إلى تطوير إستعداداتها التكنولوجية إلى جانب إستعداداتها الهجومية.

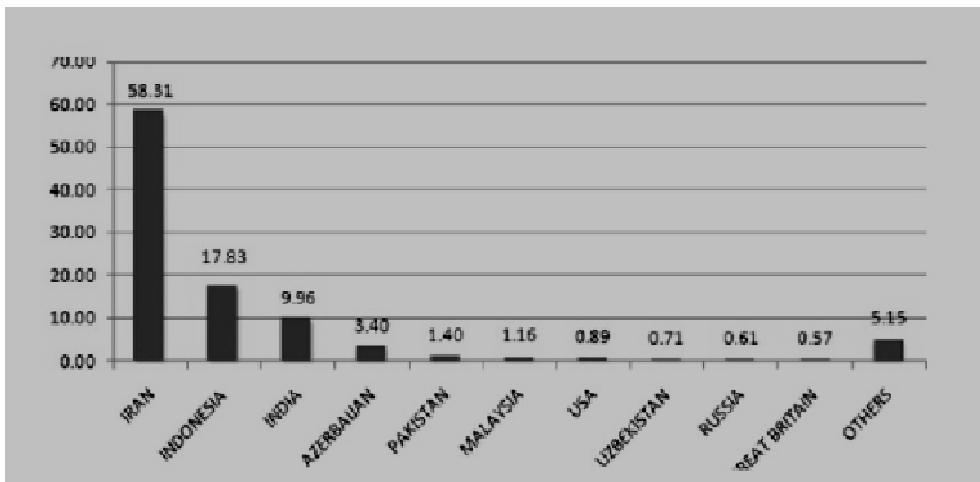
فيبريطانيا مثلاً قامت بإصدار إستراتيجية الأمن الإلكتروني القومي سنة 2009، كما قامت بإنشاء وحدة الأمن الإلكتروني ومركز العمليات ومقره مركز الاستخبارات القومية الذي بدأ عمله سنة 2010.

أما حلف الناتو فبدأ بمناقشة إمكانية اعتبار أي هجوم إلكتروني بمثابة اعتداء عسكري يوجب التدخل لحماية أعضاء الحلف، وقد ذكر تقرير الناتو في 2010 إلزامية تطوير وسائل الردع في المجال الإلكتروني.<sup>19</sup>

أما الولايات المتحدة الأمريكية بإعتبارها أكبر الدول إمتلاكا للتقنيات التكنولوجية وأكثر الدول إعتمادا على الأنترنت سواء على المستوى العسكري أم المدني فهي تسعى لتطوير قدراتها الدفاعية، ففي سنة 2009 صادق البيت الأبيض على وثيقة "مراجعة سياسة الفضاء الإلكتروني"، وبعدها كشفت وكالة الاستخبارات المركزية الأمريكية CIA عن إستراتيجية جديدة للحد من التهديدات الإلكترونية وتعزيز الأمن الإلكتروني، وفي سنة 2010 قامت بإنشاء قيادة "السايبركوم" مهمتها الحرص على حماية الفضاء الإلكتروني للولايات المتحدة الأمريكية، وهي مكونة من حوالي 1000 فرد من المحترفين في مجال القرصنة الإلكترونية.<sup>20</sup>

### ثالثاً: STUXNE كأحدث الأسلحة الإلكترونية.

من أحدث الأسلحة الإلكترونية فيروس لم يعرف مصدره إسمه ستوكست "STUXNET" ، قام هذا الفيروس بمحاجمة موقع عديدة في إيران والشرق الأوسط أشهرها المفاعل النووي "بوشهر" ، وهو ينتمل من نظام الوندوز إلى الأجهزة المرتبطة به ويظل يبحث عن أنظمة PLC وهي وحدات التحكم المنطقى القابلة للبرمجة (كمبيوتر مصغر يحتوي على عمليات برمجية فقط) والتي تعتمد على أنظمة SCADA، وعندما يصل إلى هدفه يبدأ بالتحكم وإرسال الأوامر عوض النظام الأصلي ليتحكم بذلك في ضغط الأنابيب والبخار مع إمكانية تفجير المنشأة، مع العلم أن لفيروس STUXNET قدرات تخريبية هائلة كما يوضح الشكل التالي.<sup>21</sup>



**شكل يوضح حجم الإصابة بفيروس STUXNET**

المصدر: عباس بدران، "الحرب الإلكترونية الاشتباك في عالم المعلومات"، بيروت: مركز دراسات الحكومة الإلكترونية، 2010.

وما يلاحظ من هذه الاعمدة البيانية أن إيران هي أكبر المتضررين من ستوكسنت تليها إندونيسيا والهند، مع العلم ان هذا الفيروس له قدرة تدميرية كبيرة يستطيع تعطيل حتى تفجير المصانع، فحجم الإصابة يختلف من دولة لأخرى.

#### خاتمة:

ما يمكن استنتاجه من هذه الدراسة هو أن مفهوم القوة في العلاقات الدولية قد شهد تحولات سواء على مستوى القوة او مستوى من يملك هذه القوة او مستوى طريقة قياس القوة، لظهور القوة التكنولوجية كمفهوم جديد يفرض نفسه وخاصة في مجال التطبيق في الفضاء الإلكتروني وفي الحروب الإلكترونية، لظهور بذلك وسائل جديدة للحرب كبرامج التجسس والفيروسات، مما يفرض على العالم العربي وخاصة الجزائر التفكير بجدية في مجال الفضاء الإلكتروني بإعتباره مصدر جديد من مصادر الهيديد وخاصة وإن العالم أصبح كله مرتب بشبكة الأنترنت، ويفرض كذلك وضع إستراتيجية وطنية للتطوير التكنولوجي والمعلوماتية وتقليل الفجوة الرقمية بين الدول

المتقدمة والدول العربية، وذلك من خلال تطوير الاستعدادات الدفاعية والهجومية في مجال الفضاء الإلكتروني كما يجب تطوير مجال صناعة البرمجيات العالمية والقدرة على المنافسة، وتشجيع مسار الحكومات الإلكترونية والبرلمان الإلكتروني والمجتمع الرقمي مع ضمان المشاركة السياسية والعدل ومحاربة الفساد.

ومن هذا كله يظهر ان الجزائر بعيدة جدا في هذا المجال ولهذا يجب إعادة التفكير برؤية إستراتيجية، وإدراك للواقع وللتهديدات المحيطة بنا، وكل هذا يكون بوضع المصلحة القومية والأمن القومي فوق كا اعتبار.

#### الهوامش والمراجع:

1. GARRET WARD SHELDON, **Encyclopedia of political thought**, New Yourk: Facts On File, Inc, 2001, p238
2. عبد القادر رزيقالخامي، الحرب الناعمة هل تكون بدلا لحروب المستقبل، ديوان المطبوعات الجامعية، 2015، ص 21.
3. حسين علي بحيري ، "القوى الناعمة" ، المركز الدولي للدراسات الإستراتيجية والمستقبلية ، أكتوبر 2008.
4. عبد القادر رزيقالخامي ، مرجع سبق ذكره ، ص 35.
5. محمد المهدي ، "القوة في العلاقات الدولية.....مفهوم القوة" ، موقع بحوث رؤية مختلفة ، تاريخ النشر: 17/11/2009 ، تاريخ الإطلاع: 2015/04/22 ، الموقع الإلكتروني: [www.bohothe.blogspot.com](http://www.bohothe.blogspot.com)
6. عادل عبد الصادق ، "الفضاء الإلكتروني والرأي العام" ، سلسلة قضايا إستراتيجية ، المركز العربي لأبحاث الفضاء الإلكتروني ، العدد الأول ، ديسمبر 2010 ، الموقع الإلكتروني: [www.accr.com](http://www.accr.com)
7. ربيع محمد يحيى ، "إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط" ، مجلة رؤى إستراتيجية ، 2013 ، ص 67.

- 
8. يائير كوهين، "الفضاء الإلكتروني والبعد الخامس للحرب"، ورقة بحثية مقدمة في المؤتمر الـ16 لرابطة الإنترنت الإسرائيلي، مدينة القدس، 21 فبراير 2012، الموقع الإلكتروني المتاحة فيه : [www.isoc.org.il](http://www.isoc.org.il)
9. عباس بدران، "الحرب الإلكترونية الاشتباك في عالم المعلومات"، بيروت: مركز دراسات الحكومة الإلكترونية، 2010.
10. نفس المرجع.
11. نفس المرجع.
12. محمد الحمامصي، "القوة الإلكترونية عنصر أساسى مؤثر فى النظام资料", مجلة العرب، تاريخ النشر: أبريل 2015، العدد 9895، الموقع الإلكتروني : [www.alarab.co.uk](http://www.alarab.co.uk)
13. ربيع محمد يحيى، مرجع سبق ذكره.
14. المرجع نفسه.
15. علي حسين باكير، "المجال الخامس.....الحروب الإلكترونية في القرن 21"، مقال متضور بموقع الجزيرة، الموقع الإلكتروني : [www.aljazeera.com](http://www.aljazeera.com).
16. Myriam Dunn Cavelty, "Cyberwar : concept, status and limitations, css analysis in security policy", CSS ETH ZURICH, N 71,April 2010, AT this link: [WWW.STA.ethz.ch](http://WWW.STA.ethz.ch)
17. المرجع نفسه
18. SCOTT SHACKELFORD, "A progress report on combating cyber attacks", University of Cambridge, Department of politics and international studies, journal of internet law, November 4, 2001, p 5
19. المرجع نفسه.
20. علي حسين باكير، مرجع سبق ذكره.
21. عباس بدران، مرجعه سبق ذكره.