الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة قسنطينة 3

كلية العلوم السياسة
قسم العلاقات الدولية

الرقم التسلسلي: .....
الرمـــــــــز: .....

مذكرة ماستر

الشعبة: علاقات دولية التخصص: دراسات أمنية واستراتيجية

الأمن الإلكتروني وآليات محاربة الهيمنة في العلاقات الدولية

مقدمة من طرف الطالب:
عيلان محمد رفيق

تحت إشراف:
أ. يخلف عبد السلام

الأستاذ عبد السلام يخلف	الأستاذ وليد قارة	الأستاذ صالح عميور دعاس
المشرف	المناقش	الرئيس

السنة الجامعية 2015 / 2016

الدورة: جوان

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة قسنطينة 3

كليه العلوم السياسه
قسم العلاقات الدولية

الرقم التسلسلي:.....
الرمـــــــــز:.....

مذكرة ماستر

الشعبة: علاقات دولية
التخصص: دراسات أمنية واستراتيجية

الأمن الإلكتروني وآليات محاربة الهيمنة في العلاقات الدولية

مقدمة من طرف الطالب:
عيلان محمد رفيق

تحت إشراف:
أ. يخلف عبد السلام

الأستاذ يخلف عبد السلام	الأستاذ وليد قارة	الأستاذ صالح دعاس
المشرف	المناقش	الرئيس

السنة الجامعية 2015 / 2016
الدورة : جوان

إهداء إلى:

السؤال الأول، والسؤال الأخير.

الجواب الأول، والجواب الأخير.

الفعل الأول، والفعل الأخير.

أتوجه بالشكر إلى:

الأستاذ يخلف عبد السلام الذي علمنا أن الشخص يمكنه إنجاز أي شيء إذا أدرك أنه جزء من شيء أعظم، وأن الأشخاص الذين يتشاركون هذه القناعة، يمكنهم تغيير العالم.

الأستاذ صالح دعاس، والأستاذ وليد قارة على شرف مشاركتهما لي في نقاش هذه المذكرة.

كل من كان له أثر في صناعة الشخص الذي أنا عليه اليوم.

فهرس المُحتويات

المحتويات	الصفحة
الإهداء	V
الشكر	VI
فهرس المحتويات	VII
قائمة الأشكال، والجداول، والرسوم، والخرائط، والصور	X
قائمة المختصرات	XI
0.0 مقدمة	12
1.0 إطار المفاهيم	28
1.1 أهمية المفاهيم	30
1.1.0 أهمية المصطلحات	32
1.2 الأنترنت	37
1.2.0 الشبكة العميقة	42
1.2.1 فجوة الهواء	48
1.3 الأمن	51
1.3.0 الأمن الإلكتروني	58
1.3.1 الأمن المعلوماتي	66

1.3.2 الأمن الموزع 72

1.4 الهيمنة الإلكترونية 77

1.4.0 الحرب الإلكترونية 81

1.4.1 الحرب المعلوماتية 91

1.4.2 الحرب التشفيرية 94

1.5 الرقمنة 97

1.5.0 الجيومعلوماتية 99

1.5.1 السايبرفوبيا 103

2.0 إطار نظري 108

2.1 الأمن الإلكتروني في الدراسات الأمنية 110

2.1.0 النظرية الواقعية 111

2.1.1 النظرية الليبرالية 113

2.1.2 النظرية البنائية 115

2.2 الأمن الإلكتروني والقانون الدولي 118

2.3 أساليب وآليات محاربة الهيمنة في العلاقات الدولية 124

2.3.0 الدولة والقوى الإلكترونية 124

2.3.1 الإرهاب الإلكتروني 129

2.3.2 الجريمة المنظمة الإلكترونية 131

2.3.3 الهاكتيفيزم 133

2.4 الدراسات الحربية 137

2.4.0 الجيل الأول من الحروب 137

2.4.1 الجيل الثاني من الحروب 139

2.4.2 الجيل الثالث من الحروب 141

2.4.3 الجيل الرابع من الحروب..... 143

2.4.4 الجيل الخامس من الحروب 146

2.5 السبرانية 149

2.4.0 ما بعد الإنسانية..... 154

2.6 الحقول المتداخلة 159

3.0 نماذج عن الصراع الإلكتروني الدولي 169

3.1 إستونيا 2007 171

3.2 ستوكسنت 2010 175

4.0 الخاتمة 180

5.0 قائمة المصادر والمراجع 187

6.0 الملخص ..... الغلاف

قائمة الأشكال، والجداول، والرسوم، والخرائط، والصور:

الجداول:

الرقم	العنوان	الصفحة
1.0	جدول يمثل وصفا هيكليا للشبكة العميقة	47
1.1	ترتيب الحاجيات الإنسانية، وفق طرح أبراهام ماسلو	54
1.2	جدول يوضح الأوجه الثلاثة للقوة وفقا لناي	57
1.3	شكل يوضع بعض أهم التطورات في قضايا الأمن الإلكتروني	60
1.4	جدول يوضح بعض أشكال الأخطار الإلكترونية، والأهداف التي تسعى إليها	62
1.5	جدول يوضح بعض التعريفات المقدمة للأمن المعلوماتي	69
2.0	جدول يلخص أجيال الحروب المذكورة في الدراسات الحربية	148

الأشكال:

الرقم	العنوان	الصفحة
1.0	نماذج لأنوع الشبكات وفق بول باران	40
1.1	شكل يمثل نظام الحماية عبر افصل الفيزيائي	48
1.2	شكل يمثل نظام الحماية عبر فصل فيزيائي هيكلي داخلي	49
1.3	شكل يوضح ديناميكية الأمن الإلكتروني	65
1.4	خريطة تناسبية (Treemap) تمثل الدول الرائدة في مجال الحواسيب الفائقة القدرة	80
2.0	شكل يوضح بعض التخصصات للعلماء، والباحثين، الذي شاركوا في مؤتمرات مايسي	151
2.1	شكل افتراضي يوضح تطور القوة الحاسوبية ، واقترابها إلى قيمة كرزويل للوحدة التكنولوجية	157
2.2	شكل يوضع بعض أشكال الحقول المتداخلة	165

الخرائط:

الرقم	العنوان	الصفحة
1.0	شكل يوضح أهم المراكز المالية للتداول وتنقل المعلومات من حيث المسافة بين البورصات	102

الصور:

الرقم	العنوان	الصفحة
1.0	أول شكل مشفر يمثل سكيدا 3301 (Cicada 3301)	71
1.1	أول نموذج فاعل أطلق عليه اسم المُحرر (The Liberator)	74
1.2	شعار منظمة الأمن الموزع (Defense Distributed)	75
1.3	5 أكبر مصادر لهجمات حجب الخدمة في العالم وفقا لتقرير (Akamai)	89
2.0	قطع معدنية، تمثل قيمة ثابتة لعملة البيتكوين الافتراضية، كما رمز العملة أيضا	130
2.1	أحد النماذج الأولى للغاتلين، بـ 10 مواسير إطلاق	140

2.2	أدولف هتلر - في دورة تفقدية لمدفع غوستاف سنة	142
2.3	صرب من طائرات فيرشيلد أي–10 في تشكيلة الأصابع الأربعة	144
2.4	رشاش غاتلين من نوع(GAU–8/A Avenger)؛ الرشاش الأساسي لطائرة فيرشيلد	145
3.0	صورة توضيحية لجهاز (Siemens S7-300)؛ حجمه حوالي 15*15سم	177

قائمة المختصرات والرموز:

الاختصار	الشرح
APTs	Advanced Persistent Threats
ASAT	Anti-Satellite Weapon
BRICS	Acronym for Brazil, Russia, India, China, South Africa association
CIA	Central Intelligence Agency
DARPA	Defense Advanced Research Projects Agency
DDos	Denial of Service Attack-Dos
FBI	Federal Bureau of Investigation
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
NASA	National Aeronautics and Space Administration
RAND	Research and Development Corporation
TALOS	Tactical Assault Light Operator Suit

مقدمة

> "Any sufficiently advanced technology is indistinguishable from magic".
>
> ~ Arthur Charles Clarke

إذا ما نظرنا إلى تطور المعرفة الإنسانية المدونة، يمكننا أن نرى أنه هناك تراكم معرفي على مختلف الأشكال والمواضيع، ولكن إذا ما نظرنا أكثر وتمعنا في القواسم التي تجمع هذه المعلومات المتراكمة، يمكننا أن نرى وجود أنساق مختلفة وقواعد مجسدة تُعد كثوابت أو نوًى ثابتة ومركزية من ناحية وجودها، أو من ناحية الأفكار التي تعبر عنها ومدى أهميتها بالنسبة للإنسان، ولكن في المقابل يمكننا أن نجد أن تطور كل ما يدور في فلك هذه الثوابت في تغير مستمر وهو عرضة بنسبة كبيرة للتأثر والتَغير انطلاقا من هو موجود في محيط الخارجي، ولكن رغم هذا فإن ما يتغير هنا، ليس النواة أو تلك الثوابت، وإنما الطريقة التي أصبح ينظر الناس بها إلى تلك الثوابت وطرق تحقيقها. يوضح عالم الطبيعة والجيولوجيا **تشارلز داروين** (Charles Darwin) في كتابه التعبير عن العواطف عند الحيوان والإنسان (The Expression of the Emotions in Man and Animals) والذي نشر سنة 1872 أنه هناك بعض الثوابت التي تتعلق بالطبيعة البشرية ويتكلم عن الكيفية التي يعبر بها عن بعض عواطفه، ويؤكد على أن تلك التعابير هي تعابير مشتركة بين البشر، ويقول **داروين** أن ذلك ثابت حتى عند بعض القبائل النائية التي درسها والتي حسبه لم تتواصل مع الحضارة الغربية الأوروبية من قبل؛ كما يذهب عالم الأعصاب **دوشين بولون** (Duchenne Boulogne) الذي تأثر به **تشارلز داروين** إلى أبعد من ذلك ففي كتابه ميكانيزمات الملامح البشرية (Mechanism of Human Physiognomy) الذي نشر سنة 1862؛ يضع هذا الأخير مجموعة ثابتة من الملامح البشرية التي يقوم بها الإنسان مثل الحزن أو الفرح وفقا للحركات الصغير أو الجزئية (Micro Expressions)، وبذلك فهو لا يربط هذا السلوك والتفاعل الجسدي الذي يستند إلى الملامح (Interaction Physiognomy) بعملية منظمة للتلقين السلوكي وإنما هي عملية غريزية وطبيعية في الإنسان كما هو موضح في دراسات الأنثروبولوجيا البيولوجية (Biological Anthropology) لبعض العلماء الذي تم ذكرهم والتي لها علاقة مباشرة بالسلوك الإنساني. من الواضح مما سبق أنه هناك بعض الثوابت والمزايا التي تشكل في مجملها الطبيعة الإنسانية في حد ذاتها، ولا يمكن أن تتغير بحكم أنها تجسد التركيبة الفيزيوبيولجية للجنس البشري.

كذلك الأمن؛ فالأمن يعد أحد أعقد المفاهيم التي يمكن تناولها من اجل دراسة الظاهرة الإنسانية، فمن ناحية فهو يعد ظاهرة تراكمية لها علاقة مباشرة بالمشاعر أو التقدير الذهني الإنساني لما هو حيوي أو غير حيوي ، ومن ناحية أخرى، تعد فكرة الأمن كما عرضنا سابقا أحد الظواهر الإنسانية المركزية التي لها أبعاد تتعلق بذهنيات الأفراد في فهم الأمن والعمل على تحقيقه(الشعور بالأمان وتحقيق الرغبات كسلوك مشترك بين البشر)، إلى أبعاد مادية يمكن أن تكون وسائل مادية يستعملها الإنسان لتحقيقه، أو أن تكون ظواهر مادية خارجة عن سيطرة الإنسان ولا يمكنه التحكم فيها (الظواهر الطبيعية)، بالإضافة إلى هذا يمكننا أن نرى أن الأمن يعد من المفاهيم التي لها علاقة وطيدة بالزمن وبما هو موجود حاليا، إذ أنه يتفاعل مع المدخلات التي تأتي من المحيط وتتغير وسائل تحقيقه، كما تتغير الأولويات التي كانت من قبل من المسلمات إلى أفكار جديدة وأولويات جديدة يهدف إليها الإنسان من أجل تحقيق الأمن. إلى جانب هذا يمكننا أن نرى التداخل الموجود بين الأمن ومفاهيم أخرى، إذ يمكن أن يكون هذا التداخل ذو صيغة تكاملية تلعب في نفس سياق ما يطرحه الأمن (تجاوب المفهوم مع مفاهيم مثل المصلحة والسيطرة والقوة)، أو يمكن أن يكون ذو صيغة تصادمية؛ ويعبر عن هذه الفكرة(التصادم) مثلا في تكلمه عن الديمقراطية والحرية حيث يقول القائد العسكري ورئيس الولايات المتحدة الأمريكية السابق **دويغ دايفيد ايزنهاور** (Dwight D. Eisenhower) في كتابه عهدة من أجل التغيير (Mandate for Change) الذي نشر سنة 1963:

> "**إذا أردتَ الأمن المطلق، اذهب إلى السجن. فهناك سيتم إطعامك، وإلباسك، وإعطائك الرعاية الصحية. إلى غير ذلك. الشيء الوحيد الناقص أو المفقود ... هي الحرية**".

فإذا نظرنا إلى مرور الحقبات التاريخية، يمكننا رؤية أن الأمن يعد أحد ابرز الأدوات السياسية التي استعملها الإنسان من أجل تحقيق مختلف المصالح التي يهدف إليها، وقد استمر هذا التفاعل المتبادل بين المركز (الأمن) والمحيط (مختلف التطورات التي لها اثر مباشر على تحديد الأمن) إلى الوقت المعاصر، وسيستمر مستقبلا كون الأمن له علاقة مباشرة بأبسط (من ناحية الوقاية) ما يمكن أن يؤدي إلى ضرر أو إلى نوع من الإكراه المادي أو المعنوي بين البشر، أو بين البشر والطبيعة.

من جانب آخر، وإذا ما نظرنا إلى تطور المفاهيم التي أصبح يمثلها الأمن، أي المفاهيم التي أصبحت تُعتبر كمتغيرات أمنية، يمكننا النظر إلى تطور الأساليب التي كانت معتمدة من اجل تحقيق الأمن، والتي كانت في الغالب تعتمد على الوسيلة أو الأداة الدبلوماسية، أو على الحروب كوسيلة للإكراه

المادي والمعنوي (فرض الأمر)، فقد طرأت على الأمن العديد من التحولات الجذرية؛ والتي من بينها إفرازات العديد من الأبحاث العلمية للعديد من النظريات المهمة مثل ميكانيكا الكم (Quantum Mechanics) الذي يعد العالمان في مجال الفيزياء **نيلز بورن** (Niels Bohr) و**ماكس بلانك** (Max Planck) من الأوائل الذين طوروها، والنظرية النسبية (Theory of Relativity) – النسبية العامة/الخاصة (Special relativity -General relativity) للعالم في الفيزياء النظرية (Theoretical Physics) **البرت أينشتاين** (Albert Einstein)؛ فالتركيز على هذه النظريات فقط لا يتعلق بأسباب نظرية، سياسية، ومجتمعاتية، مثل ما هو الحال مع نظريات العلاقات الدولية، وإنما هو لأسباب تتعلق بالنتائج العلمية والاختراعات الثورية التي سببتها خاصة فيما يتعلق ببعض الاختراعات التي تهمنا في مجال الأمن مثل اختراع الترنزيستور(Transistor) سنة 1925؛ يقول العالم في الفيزياء النظرية وعلم المستقبليات (Futurist) والتبسيط العلمي (Popularizer of Science / Vulgarisation Scientifique) والمتخصص في نظرية الأوتار(String Theory) في جامعة نيويورك **ميتشيو كاكو** (Michi Kaku)، في عرض على منتدى الأفكار الكبيرة (Big Think) (منتدى يقيم مقابلات مع شخصيات معروفة) :

> **"أنا فيزيائي وبعض الأشخاص يسألونني، ماذا قدمت لي الفيزياء مؤخرا ... وفي الحقيقة فنحن الفيزيائيون اخترعنا الترنزيستور، وساعدنا على اختراع الحاسوب واسعة الليزر، وساعدنا على بناء الأنترنت ... بالإضافة إلى هذا ساعدنا على اختراع الوسائل السمعية البصرية، والراديو، والرادارات، والأشعة الطبية على مختلف أشكالها... بكلمة أخرى، تقريبا كل شيء تراه الآن في الغرفة التي أنت جالس فيها، أو تراه في المستشفى؛ يمكن تعقبه إلى فيزيائي ساهم في تطويره في مرحلة من المراحل".**

فميتشيو يرى أنه من أجل معرفة المستقبل، عليك أن تفهم الفيزياء، كون الفيزياء تمثل الأساس لكل التقنيات المعاصرة أو كما يسميها العصر التكنولوجي (Technological Age)، ومن جانب آخر وفي نفس هذا السياق عبر العالم الموسوعي **غاليليو غاليلي** (Galileo Galilei) في كتابه الفاحص أو المُجرِب (**The Assayer**) الذي نشر سنة 1623 والذي يتكلم في جزء منه على الفلسفة والرياضيات، حيث قال:

"الطبيعة هي كتاب مكتوب بلغة الرياضيات".

فالعلاقة بين الطبيعة والرياضيات كانت موجودة ولكنها ترسخت بشكل أكبر مع تطور التقانة وانعكس هذا التجاذب بين الحضارة والحياة الإنسانية مع هذه التطورات العلمية على طريقة عيش الإنسان على كافة المستويات، خاصة منها ذهنية الإنسان؛ ففي عرض نفسي مصور (Psychological Thriller) يسمى بـ بيي (Pi)، والذي عُرض لأول مرة سنة 1998، وكاتبه هو دارين آرنوفسكي (Darren Aronofsky)، تصرح أحد الشخصيات، وهي شخصية ماكسيميليان كوهين (Maximillian Cohen) بهذه المقولة وهي:

"أحدد المسلمات لدي: أولا، الرياضيات هي لغة الطبيعة. ثانيا، كل شيء من حولنا يمكن التعبير عنه وفهمه عن طريق الأرقام. ثالثا، ولهذا السبب، لو عرضنا أي نظام رقميا وبيانيا، تظهر الأنساق. هناك أنساق في كل مكان في الطبيعة. (في إشارة على أن كل ما يوجد في الطبيعة له أنساق معينة ويمكن فهمها لو اكتشفنا الأرقام اللازمة، مثل ما يرمي إليه ما يسمى بتأثير الفراشة(ButterflyEffect)".

بشكل عام توضح مثل هذه الأفكار تطور الذهنيات والتصورات، التي أصبح يفكر بها الإنسان مع بداية تغير نمط عيشه، وبداية ميوله، واعتماده أكثر فأكثر على التقانة من أجل تسيير حياته. وهذا بطبيعة الحال انعكس واثر بشكل مباشرة على مفهوم الأمن وغير العديد من الاعتقادات التقليدية للأمن من عدة زوايا، كون هذه التطورات التقنية وضفت بشكل مباشرة من أجل تحقيق أو الحفاظ على الأمن بصيغته التقليدية، والموسعة؛ خاصة بعد ظهور بما يمكن تسميته برقمة الأمن (Digitalization of Security) أو رقمة الحياة الإنسانية، ويتكلم بهذا الخصوص (رقمنة الحياة الإنسانية) العالم في الفيزياء النظرية **ستيفان ويليام هوكينج** (Stephen William Hawking) حيث يقول:

"أعتقد أنه يجب اعتبار الفيروسات الحاسوبية وكأنها حية(حياة). أعتقد أن هذا يعطينا نظرة عن الطبيعة البشرية إذ أن الشكل الوحيد من الحياة التي

قمنا بخلقها (إنشائها) حتى الآن هي وإلى حد بعيد مُدمِرة بحتة. لقد قمنا بخلق شيء على صورتنا".

انطلاقا من هنا يمكننا أن نعرف بأن التقانة أصبحت توظف كأداة للإكراه الآخر، ووسيلة لتسيير الحياة البشرية، فالتطور التقني فرض نفسه على مفهوم الأمن وجعل منه، من أبرز محركات السياسة الدولية؛ فرغم أنه لن نرى مسائل أخلاقية تطرح على المستوى العلمي والتقني إلا نادرا مثلا ما هو الحال مع مسألة الحتمية (Fatalism) (Determinism) والتي يمكن أن نلخصها في مقولة ألبرت أينشتاين:

" **إن الله لا يلعب بالنرد** "

واتجاه أوائل منظري ميكانيكا الكم ضد هذا الطرح والذي يؤمن باللاحتمية (Indeterminism) والذي حاول أن يفندها الفيزيائي والفيلسوف النمساوي **إرفين شرودنغر** (Erwin Schrödinger) في طرح فكاهي يحمل اسمه، وهو طرح يسمى بـ **قط شرودنغور** (Schrödinger Cat). إلا أنه وبسبب ما يسمى بالتخصصات المتداخلة أصبح من الممكن التعاطي مع الدراسات الأمنية والعلاقات الدولية والتطورات العلمية بطريقة متكاملة، وذلك من أجل فهم أفضل وأعمق للظاهرة الأمنية عبر تفكيكها بطريقة أعمق، ومحاولة إيجاد مختلف الأعصاب التي تقوم عليها الظاهرة الأمنية.

كأحد التحولات والأشكال التي أصبحت تشكل أحد جوانب الأمن حاليا، وخاصة بعد تحول مفهوم الأمن من الطرح التقليدي، إلى الطرح الأوسع؛ يمكننا أن نتكلم على الأمن السبراني أو الإلكتروني (Cyber Security) الذي يعد كأحد أبرز فروع ومتغيرات الأمن والصراع الدولي المعاصر، فهناك العديد من النظريات السياسية التي اعتبرت الأمن كأحد أهم محددات الصراع بين الدول مثل ما هو الحال مع النظرية الواقعية، وقد عملت هذه النظريات على تقديم أجوبة على الأسئلة التي تطرح حول الأمن، وحاولت التأقلم مع مختلف التحولات التي فرضتها المستجدات الدولية، هذه التحولات طرأت أيضا على ما كان يمثله الأمن الإلكتروني، فرغم أن أنظمة الأمن الإلكتروني كانت موجودة حتى أثناء الحربين العالميتين إلا أنه ينظر حاليا إلى الأمن الإلكتروني بطريقة جدا مختلفة على التي كان عليها، وأصبح معمولا به على مختلف مستويات الحياة الإنسانية حاليا؛ فإذا كانت الفلسفة تعد أم العلوم، فالسيبرنيتيكية يمكن النظر إليها على أنها البيدق الأول في سلسة طويلة مع الاكتشافات، والطروحات الفكرية والنظرية، التي جعلت من الأمن الإلكتروني كظاهرة جديدة، جمعت بين الأنثروبولوجيا، والعلوم التطبيقية، وجعلت من الأمر حقيقة لا بد من التعامل معها بجدية من أجل الاشتراك في اللعبة الدولية.

فالأمن الإلكتروني، يشير إلى عالم أكثر تعقيدا، ويشير أيضا إلى التأثير المتزايد للتقانة في مجال التنظير في العلاقات الدولية، إذ يمكننا رؤية حدوث تقارب بين العديد من النظريات والطروحات مثل ما هو الحال مع حوار المنظورات (Inter Paradigm Debate)، في إشارة واضحة إلى أن التحولات التي طرأت على الأمن وقضايا الهيمنة والتنظير في العلاقات الدولية أصبحت تعد أكثر تعقيدا، فالنظريات أصبحت أكثر تقبلا للأفكار الأخرى والمواقف التي كانت ترفضها من قبل بشكل قاطع؛ فمثل هذه التحولات التي مست مختلف المجالات العلمية، فرضتها التطورات الكبيرة الذي حدثت في مختلف المجالات، هذا إلى جانب ما فُرض أيضا من قبل المدخلات الدولية والمجتمعاتية، وبهذا أضحى من الصعب فعلا تقدير ما يحدث وما يجب أن يكون، بدون أخذ نظرة شاملة عن ما يمثله الأمن الإلكتروني ومجمل ارتداداته وإفرازاته. فلو تكلمنا على الحروب الحديثة سنجد أن الأمن الإلكتروني اصبح يطغى بشكل كبير على عدة جوانب الحروب الحديثة مثلما هو الحال مع العتاد واللوجستية والأسلحة، كما أصبح بمثابة الحاجز الوحيد أمام أقنية الهيمنة العالمية التي تستند إلى القاعدة الإلكترونية والرقمية من أجل تحقيق السيطرة والهيمنة على الآخر، كما يجب النظر إلى أن بروز الأمن الإلكتروني، وأن الإمكانيات نفسها التي يمكن استخدامها من اجل الهيمنة العالمية، أو محاربة هذه الهيمنة، أصبحت على مستوى السلم الافتراضي والشبكي، متاحة للجميع ومعممة، ويمكن لأي شخص أن يستخدمها إذ توفرت لديه المعرفة اللازمة، الأمر الذي يوحي لنا بشكل واضح على أننا أمام شكل جديد من الحروب والصراعات والنزاعات والهيمنة، ويدفعنا في نفس الوقت إلى طرح العديد من التساؤلات في موضع الأمن الإلكتروني من واقع اليوم.

<u>إشكالية الدراسة</u>:

تعد التقانة أحد الأعصاب الرئيسية لتطور الإنسانية، كما تعد الحرب والرغبة في الهيمنة والسيطرة أحد أهم الشرايين التي تغذي الرغبة في البحث العلمي؛ فالاستخدامات العسكرية لطالما أثرت على طبيعة البحث العلمي، ومخرجاته أيضا، كذلك هو الأمن حاليا، الذي أصبح يجسد مفهوما جديد، وسط معادلة دولية مُتغيرة، ويعبر أيضا على المقاومة، ومحاربة السيطرة، وطريقة جديدة في التفكير وتقدير الأوضاع، والأحداث، والقيم، ومن هذا المنطلق، سأحاول مناقشة هذا الموضوع انطلاقا من طرح الإشكالية التالية:

فيما يكمن دور الأمن الإلكتروني، في ظل الصراع الهيمنة القائم في العلاقات الدولية ؟

بالإضافة إلى إشكالية الدراسة يمكن طرح بعض الأسئلة الفرعية:

- كيف يمكن التعاطي مع مفهوم الأمن الإلكتروني ؟
- ما هي الأشياء التي يعبر عليها الأمن الإلكتروني ؟
- فيما تكمن مختلف التأثيرات التي جاء بها مفهوم الأمن الإلكتروني ؟
- ما هي آليات محاربة الهيمنة في العلاقات الدولية في ظل ثورة المعلومات ؟
- كيف نظرت مختلف الدراسات الأمنية إلى مفهوم الأمن الإلكتروني ؟
- كيف أثرت ثورة المعلومات والأمن الإلكتروني، على البحث العلمي ؟

بناءا على طبيعة الدراسة، ومن خلال الإشكالية المطروحة، سأحاول تناول الموضوع انطلاقات من الطروحات النظري التالية:

<u>الفرضية الرئيسية</u>:

يمثل الأمن الإلكتروني، كما هو الحال مع باقي العلوم، طفرة تكنولوجية على عدة مستويات، سمحت هذه الطفرة في تغير الحياة البشرية، كما سمحت أيضا بإضافة قواعد جديدة للعبة السياسة على الصعيد الدولي؛ فالصراع الدولي المعاصر انتعش بهذه الطفرة، وجسد هذا الجيل من التكنولوجيا مفهوما جديدا للأمن، والدفاع، والصراع الدولي والبحث العلمي، وأضاف نظرة أخرى للنقاش على المستوى النظري، كما جسد أيضا جيل جديد من المشاركة الفردية في الصراع الدولي الذي لم يكن موجود من قبل.

<u>الفرضيات الفرعية</u>:

- يعد الأمن الإلكتروني مفهوما واسعا من حيث عدد الترابطات والاتصالات التي يمكن أن يجسدها مع المفاهيم أخرى، كما لديه ارتدادات عكسية من نفس هذه المفاهيم الأخيرة، الأمر الذي يدفع إلى التعامل مع مفعوم الأمن الإلكتروني بطريقة أكثر تشابكا وتعقيدا.
- يعبر الأمن الإلكتروني على مختلف المجالات السببية التي لها علاقة من بعيد أو قريب، باي قاعدة تقنية إلكترونية، فالأمن الإلكتروني يعبر على عالم جديد، عالم موازي، أصبح يعبر على كل ما يشكل الحياة الإنسانية، وتفاعلاتها في مختلف المستويات، والمجالات.

- إذا كانت الشمس تعبر على الضوء والحرارة، فإن الأمن الإلكتروني يمثل مجموعة من التغيرات الجذرية التي أتت بها ثورة المعلومات، والثورة التقنية، كما يمثل أيضا الذهنية الجديدة، وذهنية المستقبل التي أصبح يفكر بها الناس، إلى جانب طرق جديدة للعيش، وأنماط جديدة للتقدير الذهني، وأساليب جديدة للعيش والتفاعل المجتمعي، ونظرة جديدة لما يجب أن يكون عليه المستقبل.
- ثورة المعلومات والتي من بين إفرازاتها الأمن الإلكتروني، جسدت جيل جديدا من الصراع، جيل جديد تعددت فيه الفواعل الفاعلة في العلاقات الدولية، جيل جديد يضع في مقدمته قضايا الأمن الإلكتروني واستراتيجيات الدفاع الأمنية الإلكترونية، والعمل التشاركي الذي جُسد في بروز المجتمع الإلكتروني، والثقافة العالمية، بالإضافة إلى العديد من الوسائل، والأسلحة الموزعة؛ الإلكترونية منها، والغير إلكترونية، الأمر الذي جعل من لعبة الهيمنة الدولية، لعبة لم تصبح الدولة هي الوحيد التي تتقنها، وتشارك فيها.
- إن الميزة الجد تشعبية للأمن الإلكتروني، جعل من التعاطي معه جد صعب، كما أن تحسس مختلف ارتداداته على عالم اليوم يعد شيء جديدا ومعاصرا ويحتاج إلى الدراسة بشكل أكثر، رغم انه يمكن رؤية العديد من المحاولات النظرية للتأقلم كالتي حدثت مع نهاية الحرب الباردة، والتي تمكنت على الأقل من تحسس هذه الظاهرة الجديدة، ومحاولة فهمها، وتحديد موضعها من الدراسات الأمنية.
- يقوم الأمن الإلكتروني على لعديد من القواعد العلمية، كما يقوم أيضا على العديد من التخصصات العلمية المتداخلة مع بعضها البعض، فالأمن الإلكتروني يجسد في طبيعته العلمية تجمع لتخصصات متعددة، كما تطبيقاته المتعددة تجعل منه محل دراسة من قبل علماء من كل التخصصات التي يمكن تصورها، فالأمن الإلكتروني يعبر على عصر جديد عنوانه العودة إلى الموسوعية.

<u>أهمية الموضوع</u>:

لهذا الموضوع أهمية علمية تتمثل في:

- يعالج موضوع معاصر جدا، حتى وإن كانت له مرجعية تاريخية من حيث آليات قيامه، فمثل هذه المواضيع توضح لنا المستجدات الحالية فيما يخص الأمن، كما تعد عملية تحيين لفهمنا للعالم الخارجي والصراع الدولي الحالي.

- الأهمية تتركز أيضا في طرح طريقة للفهم، فمعظم وسائل الإكراه حاليا، كما معظم ما له علاقة بصنع وسائل الإكراه حاليا أصبح له علاقة مباشرة بالأمن الإلكتروني من ناحية المعدات، كما مع الأمن السبراني، إذا أخذنا بكل منظومة تسييره واستخدامه وصيانته. فدراسة هذا النوع من الأمن يشكل حلقة مهما جدا لفهم مختلف الصراعات الحالية، وعدم فهم مثل هذا النوع من التكنولوجيا ومفهوم الأمن يجعل من الصعب فهم مصالح الدول، تحديد قوتها، وتحليل مختلف التفاعلات بينها، فحاليا لا يمكن القيام بذلك مستندين فقط إلى التفاعلات السياسية.
- أما الأهمية الثالث فهي تتمثل في وضع منهج وطريقة للتفكير وتقدير المعلومات، وذلك عبر إدراج الأهمية التي أصبحت تجسدها الدراسات المتداخلة، كما المساهمة أيضا تحديد أولويات جديدة فيما يخص طريقة البحث العلمي التي تستند إلى توسيع نطاق دراسة ارتدادات القضايا وذلك من أجل نتائج أكثر دقة.
- بالإضافة إلى هذا، فهذا الموضوع يمكن أن نقول أنه فرض نفسه، فحروب السايبر أو الأمن السبراني يعد أحد محددات الحروب من الجيل الخامس، فالرقمنة طالت معظم أشكال الحياة البشرية، بداية من المعدات المستعمل، إلى طريقة إنتاج، مرورا على التصنيع، والبورصة، والغذاء و... ، لهذا فرغم أن هذا الموضوع سيركز أكثر على الأمن كوسيلة للإكراه، أو محاربة الهيمنة، إلا أن ذلك سيعطي أيضا صورة لفهم عالمنا الحالي.
- وقبل الأخير، أرى أن دراسة هذا الموضوع سيمسح، بفهم الأرضية التي تربط الدراسات السياسية وما ينطوي تحتها من نظريات، مع الجانب العلمي البحت. وذلك عبر ربط الاجتهادات النظرية التي حاولت، وقدمت تفسيرات عن طبيعة العلاقات الدولية، بمعطيات علمية من مجالات أخرى، هي تبدو بعيدة عنها ولكنها تشكل على مستوى من المستويات أحد تلك المحددات التي تستند عليها النظريات في تفسيرها للعلاقات بين البشر، فمثل ما الأمن يتغير بتغير محيطه فالنظريات تتغير أيضا بتغير مفهوم الأمن.
- أما الأهمية الأخيرة، فهي تتمثل في اعتبار مثل هذه المواضيع، مواضيع مفتاحية من أجل فهم وإدراك المحيط الدولي ومختلف تفاعلاته بشكل فعال، إذ أنه حاليا أصبح من الصعب جدا، الاعتماد فقط على الوسيلة السياسية، ففي عالم أصبح فيه الفرد يمكن أن يسبب أضرار تفوق أضرار دول بأكملها عبر شاشة حاسوبه فقط، أصبح من الواضح جدا أن

حتمية الأخذ بنظرة تداخل التخصصات يأخذ حيزا أكبر يوم بعد يوم من اجل فهم ودراسة القضايا بصورة أكبر.

<u>مبررات اختيار الموضوع</u>:

يمكن حصر الأسباب لاختيار الموضوع في:

أسباب ذاتية:

- الميل إلى الدراسات الأمنية والحروب والاستراتيجيات العسكرية وكل ما له علاقة بالحروب والتكنولوجيات بمختلف أشكالها، كما الأسلحة، والدراسات العسكرية.
- الميل إلى دراسة المعدات العسكرية، وتقنيات الإكراه، والتدريب، والفلسفة العسكرية.
- الميل إلى الدراسات العلمية بمختلف تخصصاتها، الميل إلى الموسوعية.
- الرغبة في فهم وربط المعلومات ومحاولة إيجاد أنساق وأنماط تربط مجموعة من النظم ببعضها البعض.
- الرغبة في إضافة مادة علمية ومنهجية، فكرة تسمح لأي شخص يقرأ الرسالة بأن يتنازل عن الطريقة الخطية في كسب المعلومة ويعتمد على مقاربة بين تخصصية.
- الرغبة في إخراج الدراسات الاجتماعية والسياسية من دائرة الدراسات الغير دقيقة، واعتماد لغة أكثر علمية ودقة في التعامل مع مثل هذه الدراسات.
- الرغبة في اعتماد طرح يعكس الأبواب الخلفية للصراع الدولي في الوقت الراهن، بعيدا عن اعتماد الاستنتاجات السياسية والنظرية فقط.
- الاهتمام بمعالجة مواضيع لها علاقة مباشرة بأمننا الخاص والعمل على إيجاد حلول، والتمكن من المواضيع الحالية التي لها علاقة مباشرة بالمستجدات العلمية والأمنية والإنسانية.
- الرغبة في دراسة موضوع له ارتدادات على أكبر مستقبلات مجتمعاتية، واقتصادية، وسياسية، وعلمية ممكنة.

الأسباب الموضوعية:

- انعدام شبه تام للدراسات في الأمن الإلكتروني وتطبيقاته العسكرية، وعلاقته بالتنظير في مجال العلاقات الدولية، والدراسات الأمنية.
- انعدام تام للدراسات المتداخلة خاصة بين الدراسات الاجتماعية، والدراسات العلمية المختلفة، والتي تخص قضايا الأمن، والبعد إنسانية.
- تجاوز الدراسات التقليدية لمفهوم الأمن، والأمن الإلكتروني، وذلك عبر خلق مستشعرات نظرية تسمح بخلق روابط وأدوات قياس بين ما هو علمي خاضع للعقيدة العلمية في البحوث التجريبية، وبين ما هو نظري اجتماعي.

أهداف الدراسة:

تهدف هذه الدراسة إلى محاولة تقديم وإبراز والخروج باستنتاجات تتعلق بالنقاط التالية:

- طرح كل يخص الأمن والتحولات التي طرأت عليه على المستوى النظري والتطبيقي.
- إبراز الدور الذي أصبحت تلعبه الدراسات البين تخصصية في فهم الأمن، والمواضيع السياسية بشكل عام.
- طرح قواعد اللعبة الجديدة للصراع الدولي، من وسائل تعتمد بشكل مباشر على متغير الأمن الإلكتروني، بالإضافة إلى الوسائل التي تعتمد على هذا المتغير.
- العمل على إيصال معلومات تهدف إلى الحاجة الملحة إلى تغيير وتحيين البيانات لدى الأشخاص فيما يخص الأمن وطريقة الحفاظ عليه والعمل على تحقيقه وفق ما تفتضيه أو ما تفرضه المستجدات الدولية.
- فهم قضايا الدفاع، والأمن في ظل ثورة المعلومات هذه، النظر إلى الصورة الأكبر للأحداث، وفهم أن العالم ذاهب إلى التعقيد.

صعوبات الدراسة:

يمكن حصر مجمل الصعوبات التي تم بمواجهتها لدراسة موضوع البحث في:

- الحجم المحدد للمذكرة يعد عائقا إضافيا.
- ضيق الوقت المخصص لإعداد المذكرة.
- قلة المراجع التي تدرس موضوع الأمن الإلكتروني في العلاقات الدولية، أو العلاقات الدولية في عصر التقانة.
- قلة المراجع المتخصصة في هذا الموضوع باللغة العربية، خاصة منها المعالجة المتخصصة.
- كثرة المعلومات التي يجب التعاطي معها، خاصة التي تتعلق بالجانب العلمي التطبيقي.
- معاصرة المعلومات، خاصة فيما يتلق بالدراسات البين تخصصية.
- معظم المراجع التي تعاملت معها، هي مراجع باللغة الإنجليزية، الأمر الذي اخذ وقتا إضافيا من اجل التدقيق، بالإضافة إلى انعدام تام للكتب التي تخص هذا الموضوع في المكتبة الجامعية.
- موضوع جديد، يشكل تحدي فعلي للدراسة.
- موضوع يشترط دراية وموسوعية في تخصصات علمية أخرى.
- وجود العديد من المصطلحات الغير مُعربة.
- مشاكل قهرية خارجة عن السيطرة.
- منهجية التهميش المتضاربة، التي خذت 45% من وقت إعداد المذكرة، عوض استثمارها في المضمون.

حدود الدراسة:

تهتم هذه الدراسة بمختلف الأحداث التاريخية، التي لها علاقة بالنماذج أو الأمثلة التي تخدم الموضوع، لكن الأهم هنا يتمثل في إفرازات ثورة المعلومات، والتي يشكل القرن 20 البداية لها.

المناهج المستعملة:

الطبيعة السياسية والنظرية والعلمية للموضوع تفرض استعمال بعض المناهج المذكورة كما يلي:

- المنهج الاستنباطي:

وذلك عبر الإطلاق من حالات سائدة حاليا ومحاولة العمل على دراستها وتفكيكها من أجل الوصول إلى المحركات والآليات والمكونات الأولية للأمن، والأمن السيبراني بشكل خاص.

- المنهج التحليلي:

من أجل دراسة الأمن الإلكتروني فإنه يجب اعتماد التحليل من أجل البحث على الروابط ولأنساق التي تربط الأفكار والنظريات والطروحات العلمية مع بعضها البعض. كما نقد بعض الاتجاهات السائدة حاليا فيما يخص الأمن ومحاولة تركيبها من جديد لتحاكي الواقع المعاش حاليا.

- المنهج الوصفي:

يفرض دراسة أي مفهوم أو ظاهرة، دراستها بشكل دقيق، وتوضيح الروابط الموجودة لديها، وذلك من اجل الاعتماد على حقائق فعلية موجودة ومجسدة على الأرض، كما من اجل انتقاء الظواهر والأمثلة التي تخدم البحث.

- المنهج التاريخي:

يطرح هذا المنهج أهمية كبير خاصة من اجل دراسة تطور مفهوم الأمن، كما من اجل فهم تأثير عوامل سابقة على الحاضر، بالإضافة إلى دراسة مساهمات مفكرين ومعالجة فكرة علاقة النظرية بالمنظر، وهل الواقع هو الذي يصنع النظرية، أو النظرية هي التي تصنع الواقع.

أدبيات الدراسة:

يعد معالجة موضوع الأمن الإلكتروني من بعده الأمني السياسي، شكلا نادر من الدراسات حاليا، خاصة إذا ما نظرنا للأمر من زاوية التداخل التخصصي.

هناك العديد من الدراسات الأجنبية التي عالجت هذا الموضوع من عدو زوايا، فمن جانب نجد الدراسات والكتب التي قدمها **ميتشو كاكو** (Physics of the Impossible: A scientific Exploration into the World of Phasers, Force Field, Teleportation, and time

Parallel Worlds, A Journey Through Creation, Higher Dimension, and) - (travel the Future of the Cosmos) والذي يوضح فيها التطور التكنولوجي الذي حصل، هذا إلى جانب التحديات المستقبلية الموجودة، كما تأثير ثورة المعلومات على الأفكار، والسياسة وطريقة عيشنا.

بالإضافة إلى هذا، هناك دراسات أيضا تعالج فكرة الأمن وأهم التحولات التي طرأت عليه مثل ما هو الحال مع كتاب **باري بوزان** و**لين هانسن** الذي عالج موضوع تطور الدراسات الأمنية (The evolution of International Security Studies).

بالإضافة إلى كتاب **جوزيف ناي** (Power in the Global Information Age: From Realism to Globalization) الذي تكلم على تأثير التطور العلمي والتكنولوجية على العديد من المفاهيم في العلاقات الدولية، مثل ما هو الحال مع القوة؛ بالإضافة إلى هذا وفي نفس السياق يمكن إضافة كتاب مهم لكل من **جوهان إيريكسون** و**غامبيارو غياكامالو** (International Relations and Security in the Digital Ag) الذي يركز مباشرة على موضوع العلاقة الدولية، ومدى تأثرها بثورة المعلومات.

كما يمكن إضافة مذكرة **سعيد جلعود وليد غسان**، التي تدور حول الحرب الإلكترونية في الصراع العربي الإسرائيلي، كما تكلم في هذه المكرة أيضا على تطور الحروب، ووسائل الحرب الإلكترونية.

تبرير الخطة:

في سبيل عرض المعلومات، ومحاولة الخروج باستنتاجات مفيدة، تم الاعتماد على الخطة التالية:

- إطار المفاهيم:

معالجة المفاهيم التي لها علاقة بالأمن الإلكتروني، كما المفاهيم التي كانت من إفرازات الأمن الإلكتروني، هذا إلى جانب التجاذبات الموجودة على مستوى العلاقة التي تربطه بالتطورات العلمية والتكنولوجية، كما توضيح مختلف الصيغ والعملية التي تم بها تناول الأمن على مستوى الأبحاث العلمية، إلى جانب التطرق إلى القضايا التي تتعلق بالهيمنة، وبعض المفاهيم الأمنية المفتاحية الضرورية من اجل فهم بقية الموضوع، فكل مفهوم لها علاقة سببية بالمفهوم الآخر، ويبحث الجزء الأول من الدراسة أيضا على إعطاء فكرة على ما هو ممكن في عالم الأمن الإلكتروني عبر عرض بعض الإمكانيات التقنية، وتفسيرات لبعض التكنولوجيات الموجودة، مثل ما هو الحال مع قضايا التشفير، والسايبرفوبيا، بالإضافة إلى هذا تم التطرق أيضا إلى بعض القضايا التي تبرز بعض

التحولات التي حدثت في تقدير بعض المفاهيم مثل القوة، والسيطرة، والهيمنة، والثروة، وكيفية تأثير ذلك على العلاقات الدولية.

- إطار نظري:

يتكلم الجزء الثاني على الموضوع بشكل أعمق، وذلك عبر معالجة، وعرض العديد من المعلومات المتعلقة، بالأمن الإلكتروني وموضعه من الدراسات الأمنية في العلاقات الدولية؛ وذلك عبر التركيز على بعض النظريات، مثل ما هو الحال مع الواقعية والليبرالية والبنائية. إلى جانب هذا يبحث الجزء الثاني أيضا بشكل أعمق في ما أصبح يمثله الأمن الإلكتروني والمفاهيم التي لها علاقة به بالقضايا التي تتعلق بالقانوني الدولي، وقوانين الحروب والاشتباك، بالإضافة إلى البحث في تطور الحروب، والتطرق إلى الأمن الإلكتروني في ظل هذه التطورات من اجل إيضاح أنماط التطور الذهني والتقني للصراعات، وعلاقتها بتغير الأفكار، والتقانة. ثم في الأخير البحث في الدراسات السبرانية والبين تخصصية من أجل إيضاح الطرح الذي يتكلم على العودة إلى الموسوعية وفهم الأصول الفكرية، والمنهجية التي يقوم عليها الأمن الإلكتروني الحالي، كما العديد من أفكار المستقبل التي بدأت تجسد على الأرض، والتي توضح أن أمن الإلكتروني، وثورة المعلومات، من بين المفاهيم التي ستكون في قلب النقاشات حاليا، ومستقبلا. كما محاولة طرح نظرة استشرافية قصيرة ومتوسطة المدى؛ وذلك من أجل توضيح فكرة الآليات، والأنساق المترابطة (Patterns) التي يمكن أن نعتمد عليها من أجل النظر بطريقة أخرى للمعرفة العلمية، وكيفية استخدامها، والعمل على تحسينها وتطويرها، وهذا طبعا في ظل الدراسة الراهنة والتي تتعلق بالأمن السيبراني، كأحد أشكال الوسائل المتقدمة لتسيير الحياة الإنسانية بشتى الأشكال، كما شن الحروب المعاصرة أيضا.

- النماذج:

يعالج الجزء الخاص بالنماذج، بعض الأمثلة التي تدرس حاليا في العديد من المعاهد العسكرية، وذلك من اجل إيضاح الأمن الإلكتروني وعلاقته الوطيدة بالصراعات الحالية، الإلكترونية منها، والغير إلكترونية، فقد عالجت في هذا الجزء نموذج إستونيا الشهير، وعملاق المطر، إلى جانب التكلم على دودة ستوكسنت المدمرة للمفاعلات النووية.

1.0 إطار المفاهيم

إن طبيعة الموضوع وطبيعة القضايا التي لها علاقة مباشرة بالأمن الإلكتروني، تجعل من فهم بعض الخصائص والآليات والأنظمة التي يقوم عليها الأمن الإلكتروني، والنتائج التي ترتبت عن الطفرة التكنولوجية أمرا مهما من أجل فهم الدور الذي أصبحت تلعبه تقانة المعلومات في الحياة السياسة والاقتصادية، والعسكرية، والاجتماعية، فالتطرق إلى المواضيع التي أصبحت لها علاقة وطيدة بالرقمنة أو الإلكترونيات، تعد جد صعبة، ذلك أن معالجة مثل هذه المواضيع ، وإذا ما رأينا التطبيقات أو الأنظمة الإلكترونية التي تعالجها أو التي تقوم عليها، نجد أنها من جانب أول، تعد متعددة ، وتقوم على العديد من المركبات الصغيرة التي تساعدها على العمل بطريقة فعالة، ومن جانب آخر، نجد أنها متداخلة في البناء الهيكلي الخاص بها، خاصة أنها تقوم على مجموعة من المركبات الصغيرة ذات أنظمة، وبروتوكولات متعددة ، ومختلفة تقوم عليها وتعد أساسية من أجل العمل أو تفعيل أنظمة الطوارئ عند فشل الأنظمة الأساسية. ولهذا يمكن القول أن ذلك يعد مثل كائن الإنسان، الذي يحاول دائما التطور والحفاظ على بقائه، والعمل تحقيق أمنه الخاص بأفضل الطرق ممكنة، بشكل مستمر ومتواصل، وهذا يعد أحد أهم الهواجس الحالية، تحقيق الأمن ومحاولة الحفاظ عليه مهما كلف ذلك، فهذه العملية مثلها مثل باقي التطورات في القرن الأخير، هي امتداد واضح لما كان سيقوم به الإنسان من أجل تحقيق أمنه الخاص، وبسط هيمنته على الآخر ومحاولة تحقيق الرفاهية، والاستقرار.

هذا التطور التكنولوجي، انعكس على طبيعة الصراع الذي أصبح قائم حاليا في العلاقات الدولية، وانعكس أيضا على طبيعة الاستراتيجيات المعتمدة، والأسلحة المستخدمة، بل يمكننا حتى أن نرى الانعكاسات على ذهنية الناس، إذ أصبحت هناك طريقة جديدة للتفكير يجب التعاطي معها مع أجل فهم هذي الثقافة التكنولوجية المنتشرة، فالتطور الذي حصل ساهم في خلق عالم جديد، وساهم أيضا في خلق حقول معرفية جديدة، فمن الواضح أن العالم ذاهب نحو التعقيد، أين أصبحت المشاكل اكبر من أن تعالج وفق حقل نظري واحد، كما أن الحياة السياسية أيضا رأت هذا الاعتماد الإلكتروني الذي حصل، خاصة وأن الموارد التكنولوجيا، مثلها مثل باقي التكنولوجيات التي طورت من قبل، فإن استخداماتها لطالما خضعت للدعاية والاستثمار الذي يمكن رؤيته في القضايا الاقتصادية، والاجتماعية، والعسكرية.

1.1 أهمية المفاهيم

إن القول أو الأخذ بأن العلوم الاجتماعية والمواضيع التي تتعلق بالفلسفة وعلم النفس مثلا هي مجالات لا تعد دقيقة جدا ولا يمكن التعامل مع المصطلحات والمفاهيم بطريقة موحدة ودقيقة، بسبب إما اختلاف وجهات النظر، أو النتائج المتحصل عليها بسبب البيئة، أو الخلفيات الفكرية، أو الأيديولوجية للأشخاص الذين يتعاملون أن ينظرون في هذه المجالات؛ يمكن القول من جهة أخرى أن التعامل مع موضوع الأمن الإلكتروني وتقانة المعلومات يعد عكس ذلك تماما، فبعيدا عن كل ما يتعلق بالأجهزة والأنظمة، والمصطلحات التي تحدد هذا الحقل، فقد أدت الأوضاع الأمنية التي لها علاقة مباشرة بحقل تقانة المعلومات وتأمينها إلى قناعة المجتمع الدولي وخاصة منه الصناعي، والمستخدمين الكبار للشبكات الفائقة القدرة مثل ما هو الحال مع التبادل الفائق السرعة في البورصة (High Frequency Trading)، إلى قناعة جديدة وهي العمل المشترك من أجل توحيد المعايير المستخدمة من أجل فهم أسرع وتنسيق اكبر واعتماد لغة موحدة على الصعيد العالمي، ونحن نتكلم هنا بطبيعة الحال على المقاييس أو المعايير الدولية، وبالأخص التي تضعها المنظمة العالمية للمعايير الدولية (International Organization for Standardization)، واختصارها هو أيزو (ISO).

الأيزو هي مجموعة من الوثائق التي تشمل مجموعة من الاتفاقيات والقواعد التي تتمثل في مميزات تقنية، ومواصفات فنية محددة أو معايير أخرى للجودة يتم اعتمادها كقوانين وقواعد، ومجموعة من المبادئ، والتوجيهات، والتي توضع من أجل ضمان جودة المنتجات أو المواد أو العمليات، [1] ومثل باقي العلوم التطبيقية فإنه من أجل أن يكوون هناك تواصل جيد وسرعة في التعامل مع الأخطار الأمنية، ذلك أن مثل هذه العمليات تحاول أن تطور ،وتضع مفهوم الثقة المتبادلة بين الأطراف المتعاملة مع بعضها البعض، خاصة وأن الثقة يصعب تحقيقها، ومن جانب آخر توحيد اللغة المستعملة لوصف التهديد الإلكتروني، سيساعد على توحيد وجهات النظر وتفعيل عمليات الشراكة في هذا الصدد. [2]

---

[1] Julie E Mehan, ***Cyberwar, Cyberterror, Cybercrime and Cyberactivism, an In-depth guide to the role of standards in the cybersecurity*** (United Kingdom: The Cambridgeshire business park, Published by IT Governance Publishing, 2nd edition, 2014), p. 197.
[2] ***Ibid***, p. 180.

يمكننا أن نرى هنا أن المنظمة العالمية للمعايير تحاول أن تأخذ بالعقيدة في مجال البحث العلمي والتي تقول: أن العلم لا يتقدم إلا إذا تم تقاسم المعرفة، [3] ولكن هذا طبعا لا ينطبق في جميع المجالات، كما يصعب تحقيقه أيضا، خاصة في المجالات البحثية الموجهة خصيصا للبحث على التطبيقات الاقتصادية للتكنولوجية المتوفرة حاليا، والمخابر الخاصة، والمخابر التابعة للحكومات، والمنظمات الدولية، مثل ما هو الحال مع المنظمة العالمية للصحة، ولهذا فإن هذه المحاولة هي عملية مجازفة مع هامش خطر مقبول من طرف الجميع من أجل تجنب ما هو أخطر، إذ أن الترابط الذي أصبح موجود حاليا في السوق العالمية، جعل من هذه المبادرة مقبولة من طرف الجميع إلى حد ما.

يمكن التعامل مع المنظمة العالمية للمعايير على عدة مستويات لكن الذي يهمنا هنا هو كيفية تعاملها مع التحديات التقنية في شقها الأمني، لهذا يجب أن نعرف كيفية تعامل دول العالم مع هذه المنظمة، فعدد دول المنظمة إليها وصل إلى 162 دولة لحد الآن (2016)، [4] وتصنف هذه الدول إلى ثلاثة أنواع من العضويات:[5]

1- **أعضاء الهيئة (Member Bodies)**:

وتعد هذه الدول الممثل الرئيسي للهيئة والمعايير في كل بلد، وهذه الفئة من الدول هي الوحيدة التي لديها الحق في التصويت.

2- **الأعضاء المراسلة (Correspondent Members)**:

وتمثل هذه الفئة الدول التي لا تعتمد معايير محددة خاصة بها، هذه الفئة من الدول على دراية بأعمال المنظمة العالمية للمعايير، لكنها لا تشارك في مناقشة أو إصدار هذه المعايير.

3- **الأعضاء المشتركون (Subscriber Members)**:

وتمثل هذه الفئة، الدول ذات المستوى الاقتصادي الضعيف، تدفع هذه الدول رسوما أقل للعضوية، ويمكنها متابعة التطورات التي تحدث داخل المنظمة

وطبعا يجب أن يذكر هنا أن اعتماد شهادة من مختلف شهادات الأيزو لا يعد مجانيا، فإذا أرادت أي دولة، أو منظمة، أو اتحاد، أو شركة، أو أي كان الحصول على ترخيص اعتماد شهادة الجودة مثلا

---

(3) Walter Warnick, David Wojick, " A Missing Policy: Capacity Building for Sharing Scientific Knowledge," in ***Science and Innovation Policy***, Atlanta Conference, Atlanta, GA, (2011), p. 3.
(4) Julie E Mehan, ***op. cit***, p. 181.
(5) ***Ibid***, p. 181.

في منتوج معين، يجب عليه إذ دفع مقابل مالي من أجل إجراء الرقابة وإعطائه الترخيص اللازم من أجل الحصول على شهادة الجودة، وذلك طبعا لا يكون للأبد، بل يجدد كل سنة، أو سنتين، أو ثلاثة سنوات، حسب نوع الاعتماد، فاشتراط بعض التكتلات الإقليمية مثل ما هو الحال مع الاتحاد الأوروبي شهادات جودة معينة حتى تسمح للمنتوجات بالدخول إلى الدول الأوروبية؛ جعل من الحصول على الترخيص في بعض الأحيان شرط لا يمكن الهروب منه ولا بد منه من أجل دخول السوق.

1.1.0 أهمية المصطلحات

لقد تطورت المفاهيم التي تتعلق بالأمن الإلكتروني مع مرور الوقت، وقد ساهم هذا التطور المستمر في خلق لغة خاصة في هذا المجال، كما لغة خاصة في عالم متعدد المجتمعات والثقافات، وذلك تجنبا لأي اختلاف في التعاطي مع المفاهيم، هذه الاختلافات في تحديد المفاهيم ، وتقديم شرح موحد لها، أدت في العديد من الأحيان إلى عدم وجود أرضية لفهم الآخر، وعزز ذلك الابتعاد عن الأمور الأهم التي تتعلق بالبيئة الإلكترونية والاعتماد على مقاييس معينة في الاعتماد على مصطلحات معينة من اجل التعبير على أشياء محددة، واصبح النقاش يدور حول الأصول الأنطولوجية، وكيف يمكن تحديد المفهوم الصحيح والمناسب.[6] فالصناعة المعجمية (Lexicography) وطريقة تحديد وتصنيف المفاهيم، يعد شيء مهما خاصة في العلوم التطبيقية، وتوحيدها سيدفع بالعلم إلى الأمام.

ولهذا فإن العمل على توحيد اللغة المستخدمة من أجل التعبير على مصطلحات محددة خاصة فيما يخص الأمن الإلكتروني سيسمح بوجود اتفاق وتفاهم بين مختلف الباحثين في مجال الأمن الإلكتروني، كما أن إدراج هذه المعايير في ظل مقاييس عالمية سيسمح ومع مرور الوقت بخلق وعي موحد بهذه المخاطر.

> **"هناك العديد من الخبراء الذين يعملون بشكل مستقل في مجال الأمن الإلكتروني والنتائج التي يخرجون بها يمكن أن تشكل خطرا وتحديا حقيقيا، خاصة إذا تم اعتماد معايير، ومقاييس، ومصطلحات، تم التعبير بها على شيء آخر أو على نظام آخر."**[7]

---

[6] ***Ibid***, p. 184.
[7] ***Loc. Cit***.

ولهذا يُرى أنه من الأحسن توحيد المعايير واللغة المعتمدة، ومثل هذه المقاربة لا توجد فقط في مجال أمن الأنظمة الإلكترونية، بل تمثل أحد الأسس في عقيدة البحث العلمي في العديد من التخصصات العلمية التطبيقية.

ووفقا لما سبق، يمكن القول أنه هناك مجموعة من المصطلحات المهمة والأساسية، والتي على كل متخصص وباحث في الأمن الإلكتروني أن يعرفها، كونها تعكس أهم ما يوجد في حقل الأمن الإلكتروني ويمكن تحديد أهمها في ما يلي:[8]

1. **الضمان أو الأمان (Assurance)**

وهي أرضية الأمان التي يتم اعتمادها، وذلك من اجل إعطاء التأكيد على أن المنتج أو العملية أو الخدمة التي يتم تقديمها، تتوفر على كامل الميزات والشروط الضرورية.

2. **التوفر أو الإتاحة (Availability)**

وهي الخاصة أن تكون خدمة معينة متاحة لجهة مخول لها للدخول أو استخدام ميزة معينة، وتشير أيضا إلى القدرة على البقاء في الخدمة متى طلبها أي شخص مخول له بذلك.

3. **الخصوصية (Confidentiality)**

وهو أن تكون المعلومات غير متوفرة للجميع، وأن تكون فقط متاحة للأشخاص المخول لهم ذلك.

4. **المراقبة أو السيطرة (Control)**

وتشير إلى إدارة الخطر، والتعامل مع السياسيات، والعمليات، والتوجيهات، كما التعامل مع التنظيم الهيكلي، والذي يمكن أن تكون له علاقة بالإدارة، أو بالجانب التقني، أو التسيير، أو الجانب القانوني، ويمكن أيضا أن تستعمل كلمة المراقبة على نظام دفاعي معين، أو إجراء دفاعي؛ الرقابة بشكل عام دائما تتمثل في مجموعة من العمليات التقنية، والتنفيذية، والتسييرية.

5. **السلامة (Integrity)**

وهي القدرة أو الميزة التي تهدف إلى الحرص على أن المعلومات أو البيانات لم يتم التلاعب بها أو تغييرها أو حذفها، بطريقة غير مسموح أو مصرح بها، أو بطريقة غير مرئية، أو خفية.

6. **أمن المعلومات (Information Security)**

---

[8] ***Ibid***, pp. 185-186.

وتتمثل في الحفاظ على خصوصية، أمان، وتوفر المعلومات، بالإضافة إلى أهداف أخرى مثل موثوقية المعلومات، والمسائلة (الجانب القانوني)، والتأكيد (الشهادات الرقمية)، وهندسة الوثوقية (قدرة النظام على العمل ضمن قواعد معينة) أيضا يمكن أن تدرج هنا.

7. **التأكيد أو وقف التنصل أو الإنكار (Non-repudiation)**

وتشير إلى القدرة على إثبات أنه تم القيام بفعل معين أو تم اتخاذ إجراء معين، أو إثبات حصول حدث ما، لكي لا يتم تكرار هذه العملية لاحقا.

8. **منظمة (Organization)**

ويمكن أن تكون مؤسسة، أو شركة، أو مشروع، أو سلطة، أو مركز، سواء كانت خاصة أو عامة، لديها وظائفها الخاصة، وطريقة عمل، ولديها إدارتها الخاصة، ولديها القدرة على الحرص، وتأكيد بأن المعلومات الموجودة لديها هي مؤمنة بشكل كافي.

9. **سياسة الاستخدام (Policy)**

وتمثل التوجيهات العامة التي تفرضها الإدارة على طريقة تسيير أعمالها، أو على طريقة عرض واستخدام المنتجات.

10. **المعالجة (Process)**

وهي مجموعة من التفاعلات المتداخلة والمترابطة، والتي تقوم بتحويل المدخلات إلى مخرجات. المدخلات في عملية معينة، تمثل المخرجات في عملية أخرى. عملية المعالجة في منظمة ما، تقام في العادة تحت رقابة وظروف محكمة، وذلك بسبب القدرة على إضافة قيم معينة أثناء هذه العملية وهو الأمر الذي يجعل منها عملية خطيرة.

11. **المخاطرة أو الخطر (Risk)**

وتشير إلى احتمال أن تهديد ما أو جهة ما ستقوم باستغلال ضعف أصول معينة أو مصادر معينة، هذه الأصول أو المصادر، يمكن أن تكون مصدرا للثروة، أو الاستغلال الغير القانوني، ويمكن أن تكون لأي أغراض تهدف إليها جهة معينة. هذا النوع من المخاطر سيسبب أضرار كبيرة للمنظمة، وعملية قياس المخاطر، تتم عبر الجمع والمقارنة بين احتمال حدوث الخرق، والنتائج التي يمكن أن تترتب عنه.

12. **إدارة المخاطر أو الخطر (Risk Management)**

وتتمثل في تنسيق الأعمال والأنشطة، من أجل إدارة المنظمة لما يتعلق الأمر بخطر محتمل، إدارة الخطر يتضمن في العادة إعادة تقييم الأوضاع الراهنة، معالجة وتحليل الخطر، إدراك الخطر الفعلي، ثم التبليغ عن الخطر.

13. الأمن (Security)

ويتمثل في جميع الجوانب التي لها علاقة بالحفاظ على الخصوصية، والسلامة، والتوفر، ووقف التنصل، والمسائلة، والصحة، والموثوقية.

14. الخطر (Threat)

وهي قدرات، نوايا، طرق وأساليب هجوم العدو، أي ظرف أو حدث، أكان من مصدر خارجي أو داخلي، تكون لديه القدرة على التسبب بأضرار للمعلومة، أو البرنامج، أو النظام.

15. الثقة أو الائتمان (Trust)

وهي علاقة بين عنصرين، أي مجموعة من الأنشطة والسياسات الأمنية التي يتم اعتمادها، والتي يثق فيها العنصر أ بالعنصر ب إذا وفقط إذا كان للعنصر أ ثقة تامة في أن العنصر ب سيتعامل بطريقة محددة مسبقا، وأن هذه الطريقة لن تخالف أو تنتهك السياسة الأمنية.

الضعف أو قابلية الإصابة (Vulnerability)

وتعبر هذه النقطة عن ضعف في نظام المعلومات، نظام الإجراءات الأمنية، الرقابة الداخلية، أو في إدراج أو حقن معين يمكن أن يتم استغلاله عبر تفعليه من قبل التهديد.

يجب أن نعرف أن هذه المعايير، والمصطلحات المقدمة، ليست نهائية، بل توجد هنا معايير أخرى، متخصصة في أنظمة معينة للحماية، ومن جانب آخر، صحيح أن ممعيرة المصطلحات وطريقة العمل المعتمدة، وتقاسم المعلومات، ووضع أرضية من أجل تسهيل عملية التواصل والتبادل، تساهم بشكل كبيرة في تسريع وتيرة البحث عن طرق جديدة للحماية، وترصد الأخطار، إلا أنه من جانب آخر هناك العديد من الطروحات التي تقول بالصعوبات الكبيرة من أجل تحقيق، وتوحيد هذه المعايير، ويمكن ذكر الأسباب المقترحة فيما يلي:[9]

1. وجود عدد كبيرة من المعايير، وذلك جعل من الصعب جدا التعامل مع العدد الكبيرة والمتزايد للمعايير والمقاييس التي تتعلق بالأمن الإلكتروني، فإدراج البرامج المتعلق بتحديث أنظمة الدفاع الإلكتروني، سواء داخل الدول أو المنظمات على مختلف أشكالها، تعد عملية صعبة وليس من السهل تحقيقها، بسبب المتطلبات العديد التي يجب أن تتوفر، مثل ما هو الحال مع الإمكانيات المادية، واللوجستية.

---

[9] ***Ibid***, pp. 193-191.

2. صعوبة كبيرة من أجل تحقيق المقاييس: فقد كانت هناك انتقادات كبيرة تتعلق بالتوجهات المتعلقة بـ ISO/IEC 27001 والتي لها علاقة بالأمن الإلكتروني والأنظمة التي يجب تحديثها، ولكن طرحت هناك العديد من المشاكل فيما يخص أن التوجيهات المقدمة لم تكن واضحة بشكل كافي، أو لم توفر المادة الفنية الكافية من أجل تحقيق شروط الشهادة.
3. يتم اعتبارها في العديد من الأحيان على أنها غير ديناميكية، إذ أن مثل هذه الشهادات والمقاييس يجب أن يكون لها تحديث مستمر، ولكن بعض التوجيهات، والشهادات لا يتم تحديثها إلا مرة كل خمسة سنوات، مما يجعل الأمر صعبا جدا من اجل جمع المعلومات، وتحليلها.
4. المقاييس المقدمة لا تشكل ضمان، ولهذا هناك فكرة حول أنه لا يجب اعتبار المعايير المقدمة، كضمان تام للأمن الإلكتروني، خاصة إذا أصبح الأمر شبيع بالتبعية لمثل هذه المعايير، ولهذا من الأحسن تفعيل إجراءات رقابة مستمرة، وتحليل المعلومات من طرف الدول نفسها أو المستخدمين أنفسهم من أجل خلق سلوك تنظيمي يهدف إلى تفعيل الحرص، والرقابة المستمرة.
5. إشكال آخر وهو أن تفعيل، وإدراج هذه المقاييس يتطلب موارد، واستثمارات، ووقت أيضا، مثل ما هو الحال مع الاستثمار في الطاقة، والموارد، والوقت، فلكي تكون عملية الإدراج ناجحة، ومن اجل أن يكون الاستثمار ناجح، يجب أن يكون مستقر ومستمر. وفي الحقيقة، السبب الأساسي في فشل تحسين نظام الأمن الإلكتروني في العديد من المرات، يتمثل في ضعف الاستقرار والالتزام بما يتطلبه الأمر.
6. المقاييس توفر "ماذا" ولكنها لا توفر "كيف"، فالاستراتيجيات المعتمدة فيما يخص تطبيق المقاييس، نادرا ما تقدم توجيهات دقيقة من أجل الإدراج، حتى أنه هناك العديد من المنظمات يمكن أن تعتمد على مقاييس معينة على حساب مقاييس أخرى بطريقة غير صحيحة، الأمر الذي يؤدي بها إلى إنفاق إضافي غير ضروري. وفي ظل هذا المستوى من التعقيد والصعوبات، يمكن للعديد من المنظمات أن تعمل على تحقيق وتلبية شروط الاستخدام فقط للحصول على الشهادة، والمقاييس، ولكنها بهذه الطريقة تبتعد عن الغرض الحقيقي من المبادرة، وهو تحقيق الأمن الإلكتروني الخاص بها، ونشر الثقافة الأمنية.
7. المعايير أو المقاييس في حد ذاتها لا تعد حلا سحريا، فالمنظمات تعد بمثابة أنظمة معقدة وإدراج هذه المقاييس بشكل تام لا يعد أمرا سهلا، ففي ظل هذه البيئة المتغيرة، يمكن القول أن المقاييس لا تعد حلا سحريا من اجل تحقيق الأمن الإلكتروني، فهناك بعض المقاييس التي لا يمكنها أن تتوافق مع بعض الممارسات التجارية لمنظمة معينة أو مع مستوى الثقة المطلوبة التي تفرضها المقاييس، مثل ما هو الحال مع تبادل المعلومات التي تتعلق بالأمن ومستويات الدفاع، فالبيانات في عالم الأمن الإلكتروني تعد

عاملا مهما في فهم طريقة عمل أي نظام أمني، كما فهم أي الطرق تم اعتمادها من أجل محاولة اختراق أي نظام.

1.2 الأنترنت

من أجل فهم ما تمثله الأنترنت في مجال الأمن الإلكتروني، يجب علينا أولا التفريق بين المفاهيم والمصطلحات، خاصة منها التي تستعمل بطريقة غير صحيحة؛ إذ هناك من يستعمل كلمة الأنترنت (Internet)، ككلمة لها نفس معنى الفضاء الإلكتروني (Cyberspace)، ولكن هذا ما بحثنا عن المعاني الدقيقة لهذه المفاهيم، يمكن أن نجد أنها تعبر على أشياء مختلفة، حتى لو كانت، وعلى مستوى ما، مترابطة إلى حد كبير جدا، من حيث المعنى، أو من حيث الوظيفة، أو من حيث اعتبار مفهوم ما جزء من الآخر، أو العكس.

يعد الفضاء الإلكتروني، مفهوما حديثا، إذ يعد الكاتب المتخصص في روايات الخيال العلمي **ويليام غيبسون** (William Gibson)، أول من أشار إليه في رواية نيرومانسر (Neuromancer) سنة 1984، والتي تكلم فيها على قضايا الذكاء الصناعي، والجينات، وتبادل المعلومات، والمصفوفة (The Matrix)، وقضايا تتعلق بالسايبربنك (Cyberpunk)، والشركات المتعددة الجنسيات، و*الشركات الفائقة القدرة (MegaCorporation - Megacorp)، وقد عبر ويليام غيبسون عن الفضاء الإلكتروني في كتابه، حيث قال:[10]

> "**الفضاء الإلكتروني، هو بمثابة شبكة افتراضية، تقوم بربط كافة البيانات الرقمية التي يمكن الوصول إليها، والتفاعل معها، عبر أي حاسوب مربوط بالشبكة**".

فعند ربط مجموعة من الحواسيب ببعضها البعض، وتكون هناك إمكانية للتفاعل مع المحتوى التي تم عرضه، يكون هناك ما يسمى بالفضاء الإلكتروني، فمثل ما يتم تصميم الألعاب الإلكترونية بطريقة

---

[10] Robert M Kitchin, "Towards Geographies of Cyberspace," in ***Progress in Human Geography***, No 3, volume 20 (June, 1998.), pp. 385-406.

- الشركات الفائقة القدرة (MegaCorporation): أحد القضايا التي طرحها ويليام غيبسون، ويرمي بهذا المصطلح، إلى شركة، أو تكتل اقتصادي خاص(Conglomerate)، مثل أن يكون لشركة ما قوة فائقة تتعدى قوة الدولة، وبهذا يكون لديها جيش خاص، وعقيدة خاصة، ولا يوجد لديها أي احترام فعلي لأي قانون خارجي.

ثلاثية الأبعاد تسمح للاعبين بالتجول بداخل العالم الافتراضي الذي تم خلقه، يمثل الفضاء الإلكتروني نفس الفكرة، فهو يعبر على العالم الموازي الذي تم خلقه، والذي بداخله، تتم مختلف التفاعلات التي تحصل في الشبكة، وبعيدا كل البعد عن أي مفهوم للزمن، والمسافة، والحدود، وقد عُرضت هذه المعلومات خاصة عندما تم التكلم عن ما يسمى بالمواطن الإلكتروني (Netizen)، كفكرة تعبر عن الدور الذي أصبحت تلعبه الأنترنت في الحياة الإنسانية، وقد عبر على ذلك **ميكاييل هوبن** (Michael Hauben 1973-2001)، الذي كان يدرس تأثير التكنولوجية والأنترنت على الحياة الاجتماعية، حيث قال:[11]

> "**تعيش في عالم لم يعد فيه الزمن، أو الجغرافيا بمثابة حدود، عالم أصبحت فيه الاختلافات الاجتماعية والسياسية لا تشكل عائقا أمام الصداقة والعلاقات بين المجتمعات، فبهذه الطريقة، أصبح أي مواطن إلكتروني يمكنه أن يقابل مواطن إلكتروني آخر في أي مكان في العالم، ما كان ليقابله لول الشبكة**".

فقد اعلن في هذا العصر، على أن الجغرافيا قد انتهت، خاصة بمفهومها المكاني المتعلق بتنقل المعلومات والتواصل مع الآخر، فقد تغيرت الذهنيات في ظل وجود هذا العالم الموازي والمجهول، إذ أنه لا توجد جهة معينة تسيطر على هذا العالم، ويمكن لأي شخص أو مواطن إلكتروني، أن يساهم بطريقة أو بأخرى في تحديد معالم هذا العالم الإلكتروني، وهذا ما أكده المهندس، والمصمم، والباحث في القضايا الحاسوبية **ويليام جون ميتشل** (William Jon Mitchell 1944-2010)، حين قال:[12]

> "**يعد الفضاء الإلكتروني، وبشكل عميق، مضادا لمفهوم الفضاء ببعده الجغرافي التقليدي، فالفضاء الإلكتروني، لا يمكنك تحديد مكانه، ولا يمكن تحديد حدوده، أو حجمه أيضا، فقد تجد أشياء تبحث عنها، ولكنك لا تدري أي هي بالتحديد، فالشبكة هي بمثابة مناخ، لا مكان له بالتحديد، ولكل في كل مكان في نفس الوقت، لا يمكن الذهاب إليه، ولكن يمكن الدخول إليه عبر أي جهاز فيزيائي كفيل بذلك.**"

---

[11] Michael Prosser, K.S Sitram, Civic Discourse , **Intercultural, International, and Global Media** (The United States of America, Stamford, published by Ablex Publishing Corporation, the first edition, volume 2, 1999), p. 51.

[12] William J. Mitchell, ***City of Bits: Space, Place, and the Infobahn*** (The United States of America: Massachusetts, published by MIT Press, the first edition, 1996.), P. 10.

من هنا يمكننا أن نرى، أنه ما يمثل الفضاء الإلكتروني، هو المناخ، أو العالم الذي يشعر الشخص أنه موجود، العالم الرقمي الذي أصبحت له قيم معينة تحدد ما يوجد به، وكيفية التعامل معه، فالفضاء الإلكتروني، أصبح يمثل كل ما هو افتراضي وله علاقة وطيدة بما توفره الأنترنت، هذا المناخ، أو القواعد الأولية، سمحت للعامة بتكوين صورة ذهنية حول الفضاء الإلكتروني، ولكن الأهم هو فهم حقيقة أن هذا الفضاء كانت له العديد من الإفرازات على العالم المُعاش، وقد غير في العديد من المواضع، طريقة رؤيتنا للسياسة، والاقتصاد، والأمن، والعديد من مجالات الحياة الإنسانية.

تعود أول إشارة إلى ما سيسمى لاحقا بالأنترنت، إلى العالم الأمريكي في الحاسوب، **جوزيف كارل غوبنات ليكلايدر** (Joseph Carl Robnett Licklider 1915-1990)، حين أشار في المقال الذي نشره سنة 1962 تحت العنوان (On-line Man-computer Communication) إلى فكرة إمكانية التواصل الاجتماعي عبر استخدام شبكة من أجل إرسال المعلومات. [13] من جانب آخر هناك من يرى أنه لا يمكن تحديد أصل الأنترنت بدقة، ذلك أن مكوناتها كانت نتيجة تراكم واجتهاد العديد من العلماء في العديد من التخصصات، وفي حقبات زمنية مختلفة. [14]

ولكن رغم ذلك، ومما لا شك فيه، يمكن القول أن الفضل الأكبر في بناء الأنترنت بالصورة التي نعرفها اليوم، يعود إلى ثمرة الأبحاث التي قامت بها شبكة وكالة مشاريع البحوث المتقدمة الأمريكية (Advanced Research Project Agency Network - ARPANET) ، فقد اطلق مشروع سنة 1966، وقد كان الهدف الأساسي من هذا المشروع، هو إيجاد طريقة فعالة، من اجل ربط كافة القوات، والقيادات العسكرية الأمريكية، بطريقة اتصال، تسمح بالتمرير السريع والآمن، للأوامر، والمعلومات، والقرارات النهائية لمؤشرات *ديفكون لتقييم الخطر (The Defcon Protocols)، كما مساهمة وكالة

---

[13] Joseph Carl Robnett Licklider, Welden E. Clar, "On-line Man-Computer Communication," in ***American Institute of Electrical Engineers-IRE***, Spring Joint Computer Conference (May 1-3, 1962), pp. 113-128.

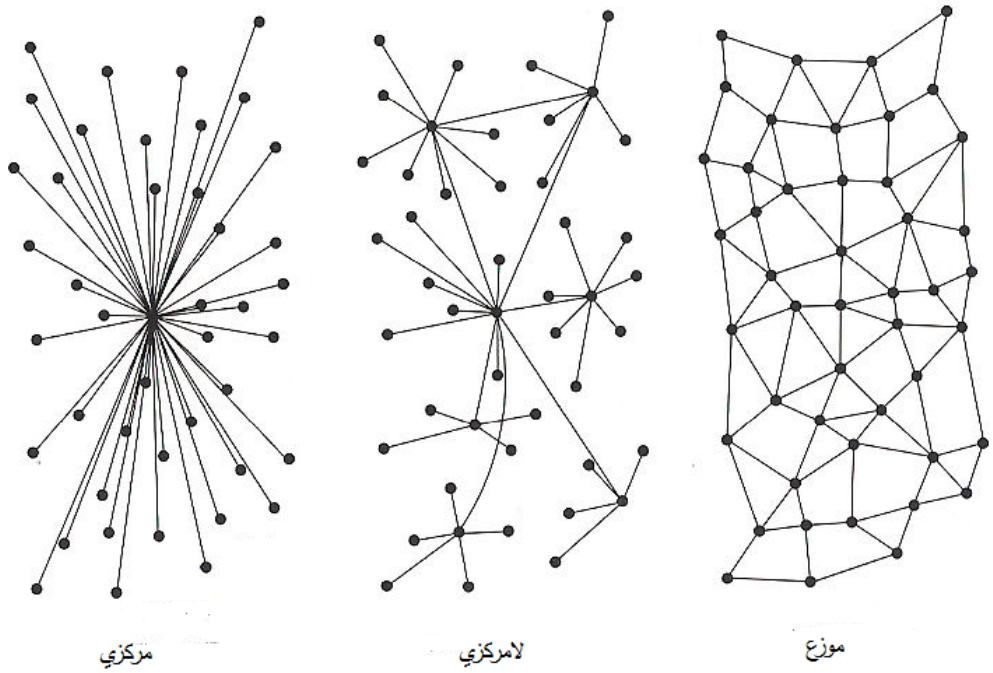
- ديفكون (Defcon): نظام بدأ استعماله سنة 1959، ويعد بمثابة مؤشر للاستعداد العسكري الذي تستعمله الولايات المتحدة الأمريكية، به 5 مستويات؛ المستوى الخامس يشير إلى تجهيزات في وقت السلم، المستوى الرابع يشير إلى تجهيزات عادية مع استطلاع أكبر، المستوى الثالث يشير إلى زيادة في تجهيز الجيش، المستوى الثاني يشير إلى مضاعفة تجهيز الجيش، والمستوى الأول يشير إلى اقصى تجهيز للجيش ويشير أيضا إلى حالة حرب نووية أو على التراب الأمريكي. أقصى مستوى وصلت له هذه المستويات هو المستوى الثاني، وكان ذلك أثناء الآزمة الكوبية.

[14] Leonard Kleinrock, "An early History of the Internet," in ***IEEE Communication***, No 8, volume 48(August, 2010), P. 26-36.

مشاريع البحوث المتطورة الدفاعية (Defense Advanced Research Projects Agency)، الأمر الذي يوضح لنا، أن البدايات الأولى للأنترنت، كانت لأغراض عسكرية.[15]

يجب أن نعرف هنا، أن مبدأ عمل الشبكات الإلكترونية، أي ربط مجموعة من الأنظمة مع أجل أن تعمل معا بشكل متكامل، لا يعد أمر جديدا جسد فقط في الستينات، بل كانت هناك العديد من الأنظمة التي كانت تعمل بطريقة موزعة، مثل ما هو الحال مع أنظمة الاتصال التقليدية، أو أنظمة الرقابة والترصد.

الشكل رقم: 1.0



نماذج لأنواع الشبكات التي عرضها العالم في الفيزياء، والحاسوب،

والرياضيات **بول باران** (Paul Baran 1926-2011) سنة 1960. [16]

---

[15] Barry M.Leiner, Vinton G.Cerf, David D.Clark, Robert E.Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Posteln Larry G.Robertsn Stephen Wolff, "A Brief History of the Internet," in ***SIGCOMM Computer Communication Review***, No 5, volume 39 (October, 2009), pp. 22-31.

[15] Paul Baran, ***On Distributed Communication, Introduction to Distributed Communication Networks*** (The United States of America: published by the Rand Corporation, 1964), p. 2.

يمكننا أن نرى في **الشكل 1.0**، أن **بول باران**، يعرض مجموعة من النماذج الشبكية سنة 1960، والتي لا زال يستخدم حتى الآن. فحاليا، تستخدم الولايات المتحدة الأمريكية، وبقية دول العالم التي تعتمد على ما يسمى بالانتخابات أو عمليات الاقتراع الإلكترونية، على النموذج الشبكي الموزع الذي عرضه بول باران، إذ أن استخدام النموذج المركزي، من شأنه أن يزيد فرص التزوير لأنه توجد فقط سلطة أو هيئة مركزية ستقوم بعملية الرقابة، عكس النموذج الموزع، والذي يعتمد على عدة أماكن من أجل تأكيد النتائج، فأي عملية اقتراع، يمكن تأكيدها من عدة أماكن، الأمر الذي سيقلل من فرص التزوير بشكل كبير، لأنه من المستحيل إدراج نتائج لم يتم تأكيدها من قبل جميع الشبكات المشاركة في العملية الانتخابية. الأمر الذي نريد توضيحه هنا هو أنه حتى لو أن النماذج الحالية تعد بعيدة جدا على النماذج التقليدية، إلا أنه يمكن فهمها عبر هذه النماذج البسيطة، والتي لا زالت تعد أحد أساسيات عمل الشبكات في الوقت الحالي.

وفي 24 أكتوبر 1995، أعلن مجلس الشبكات الاتحادي (Federal Networking Council)؛ وهو مجلس مفوض من قبل المجلس الوطني للعلوم التكنولوجية الأمريكي (National Science and Technology Council)، الذي هدفه الأساسي هو مناقشة القضايا التكنولوجية وضبط المفاهيم وتوحيدها، وهذا ما حدث فعلا حين تم الاتفاق بالأغلبية المطلقة على مفهوم الأنترنت، وكان التصريح كما يلي:[17]

> **"يوافق مجلس الشبكات الاتحادي، على أن المفاهيم التي ستطرح، هي مفاهيم تعبر على مصطلح الأنترنت، ولهذا، فالأنترنت تشير إلى أ. عملية ربط منطقي، عبر عنوان واحد قائم على بروتوكولات الأنترنت (IP)، ب. القدرة على دعم وإقامة الاتصال عبر استخدام ميفاق ضبط الإرسال (TCP-IP)، أو أي امتدادات آخر يمكن استخدامه، ج. توفير خدمات، سرية، أو علنية، عبر استخدام بنى الاتصالات التحتية والمختلفة."**

---

[17] Barry M.Leiner, Vinton G.Cerf, David D.Clark, Robert E.Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Posteln Larry G.Robertsn Stephen Wolff, **Op. Cit**. pp. 22-31.

أما حاليا، فالشبكة التي نعرفها الآن بصيغتها الأكثر تبسيطا وتوفرا، فقد برزت خاصة مع إنشاء ما يسمى بالشبكة العنكبوتية العالمية (World Wide Web) بداية التسعينات، وقد كان للمنظمة الأوروبية للأبحاث النووية (The European Organization for Nuclear Research - CERN) دور البيدق في هذه العملية، إذ أن المنظمة أرادت نشر الوثائق والمعلومات بين المراكز البحثية، عبر استخدام ما يسمى بالنص التشعبي (Hypertext)، بعد 1994، وخاصة مع بروز واجهات المستخدم الرسومية التفاعلية (Graphical User Interface)، أصبح الشبكة في توسع مستمر، وانتقلت من مراكز البحث والشركات، إلى الاستخدام الشخصي الموسع.[18]

من هنا، يمكننا أن نرى أن الفضاء الإلكتروني يعبر عن تلك العملية التي تقوم بربط البيانات ببعضها البعض، وبطريقة تسمح بخلق عالم افتراضي يمكن التفاعل بداخله مع مختلف البيانات المتواجدة فيه، كما التفاعل مع المواطنين الإلكترونيين الآخرين، في ظل تبادل للمعلومات وتفاعل مستمر، وبطريقة توحي فعلا بوجود عالم موازي يمكن للشخص فيه، أن يقوم باي شيء، بداية من تحقيق أمنه الخاص، مرورا بتحقيق المصالح المالية والسياسية ومختلف مصادر الفائدة، إلى التسبب بالضرر وإلحاق الأذى بالآخر. من جانب آخر يمكن ربط الأنترنت، بكل ما يتعلق بالجانب الفيزيائي، والمنطقي، والعملياتي، لتسيير الشبكات، ولكن، العلاقة الموجودة بينهما هي علاقة سببية، وهيكلية، وحتمية، كالجسم الذي يحوي الدماغ، والدماغ الذي يوفر المخيلة.

1.2.0 الشبكة العميقة

يمكن النظر إلى الأنترنت على أنها عالم افتراضي متكامل، هناك أماكن يمكن الوصول إليها، ولكن من جانب آخر هناك أمان سيصعب الوصول إليها، ومن أجل الوصول إليها، يجب أن تتوفر مجموعة من الأدوات، أو المعرفة الفنية من اجل القيام بذلك، فعند ولولج أي شخص إلى الشبكة، فهو يضن أنه في عالم مفتوح، حيث أنه يمكن أن يذهب حيثما يريد، لكن الحقيقة غير ذلك، إذ انه بغض النظر عن الحجب التي تقوم به العديد من الدول على الأبحاث العلمية، والمادة التي يمكن للعالم الثالث أو المتخلف الاستفادة منها، هناك عالم آخر يعبر على الشبكة الحقيقية كونها تحوي الجزء الأكبر من بيانات الشبكة،

---

[18] Tim Berners Lee, Robert Cailliaud, Ari Loutonen, Henrik Frystyk Nielsen, Arthur Secret, "The World Wide Web," in ***Communication of the ACM***, No 8, volume 37(August, 1994), pp. 76-82.

فإذا كان العالم الافتراضي المتاح توجد به قوانين صارمة نوعا ما، مثل ما هو الحال مع القوانين التي تفرضها المنظمة الغير ربحية آيكان (ICANN)، أو بروتوكول طبقة المنافذ الآمنة (Secure Socket Layer - SSL) والتي يفرض مستوى عالي من الأمن في تنقل المعلومات في المواقع، والرقابة الخاضعة لصلاحيات قانونية من قبل الدول، مثل ما هو الحال مع حق الحصول على معلومات أو الهوية عند تقدم حكومات بعض الدول بذلك، فإنه من جانب آخر يمكن القول، أن الشبكة العميقة، أو المظلمة، تمثل عكس ذلك تماما.

فالشبكة العميقة تشير إلى أي محتويات لم تتم فهرستها من قبل محركات البحث لعدة أسباب ممكنة، وتمثل أيضا أي شبكة لا يمكن الدخول إليها عبر استخدام الوسائل التقليدية، أو الإعدادات التقليدية التي يستخدمها المستخدم العادي من أجل الولوج إلى الأنترنت، فالمستخدم العادي لن يتمكن من الدخول إلى المواقع التي لم تتم فهرستها، أو المواقع التي لم يتم تسجيلها وفق القوانين المعمول بها لإنشاء أسماء النطاقات (Domain Name)، عكس أسماء النطاقات التي تنتهي بـ Onion. فإن هذا النوع من النطاقات لا يخضع لقوانين آيكان، وله استضافة لامركزية مما يجعل من الصعب تتبع الأشخاص أو مصدر الموقع.[19]

تمثل الشبكة العميقة حوالي 99% من البيانات الموجودة على الأنترنت، ولكن معظم هذه البيانات مخزنة في قواعد بيانات ولا يمكن الولوج إليها بسبب الفهرسة كما وضحنا ذلك سابقا، لذا يجدر القول هنا، أن الإبحار في الشبكة العميقة كان موجها فقط للمتخصصين، وللذين لديهم معرفة متقدمة في الإعلام الآلي وطريقة عمل الشبكات، أما الآن، فقد برزت هناك العديد من محركات البحث، التي وظيفتها الأساسية هي فهرسة الشبكة العميقة، الأمر الذي سمح بظهور بما يسمى بـ (The Hidden Wiki)، وهي مواقع يوجد بها أرشيف بها أهم المواقع الموجودة في الشبكة العميقة، أهم محركات البحث أيضا، وبذلك اصبح أي شخص لا توجد لديه أي معرفة تقنية، أن يقوم بتحميل متصفح تور (Tor) ويبحر في الشبكة العميقة، ولكن ذلك طبعا على حساب سلامته الخاصة.[20]

---

[19] Vincenzo Ciancaglini, Marco Balduzzi, Robert McArdle, Martin Rösler, **Below the Surface: Exploring the Deep Web** (The Global Technical Su pport and R&D, Center of TREND MICRO, published by Trend Micro, 2015), p. 5.

[20] Steven R Gruchawka, ***Using the Deep Web: A How-To Guide for IT Professionals*** (techdeepweb.com, published by Steven R Gruchawka, 2005), pp. 2-8.

- هايدرا (Hydra): وحش أسطوري من الميثولوجيا الإغريقية، لديه عدة رؤوس، يخلق له رأسين مكان كل رأس يتم قطعه.

لكن هناك سؤال يطرح هنا، وهو محاولة معرفة الأسباب التي يمكن أن تدفع شخص إلى الدخول إلى الشبكة العميقة، أو السبب الذي يمكن أن يدفع شخص إلى إنشاء موقع على الشبكة العميقة؛ لقد قلنا من قبل أنه هناك العديد من الأسباب التي يمكن أن تدفع محركات البحث المعروفة مثل محرك غوغل (Google) إلى عدو فهرسة الشبكة العميقة، ومن بين هذه الأسباب، هي طبيعة المضمون الذي ينتشر في الشبكة العميقة، فمجرد الدخول إلى الشبكة العميقة، يمكن إيجاد مواقع لبيع المخدرات، الأعضاء البشرية، التجارة البشرية، بيع وشراء الأسلحة، قتل الحيوانات، قتلة مأجورين، قراصنة مأجورين، مواقع التشفير، تسريبات للوثائق السياسية، فضائح، بيع وشراء البطاقات البنكية المسروقة (Visa / Master Card)، العنف ضد الأطفال، النشطاء الرقميين، بيع وشراء الوثائق المزورة، بيع وشراء المواد الكيماوية، بيع وشراء الحيوانات المعرضة للانقراض، بيع وشراء أشرطة الابتزاز، تحميل غير قانوني للملفات على مختلف أنواعها؛ بشكل عام، كل نشاط غير قانوني وأخلاقي وإنساني يمكن أن يمارس عبر الشبكة لذر الأرباح أو تحقيق مصالح معينة، يمكن إيجاده في الشبكة العميقة بطريقة سهلة ومتاحة للجميع، لكن العملية خطرة في حد ذاتها، لأنه لا توجد هناك أي حماية، كما يمكن أن يتعرض الشخص لعقوبات قانونية قصوى في حالة ما إذا كان يستغل محتوى غير قانوني، أو تم الإيقاع به من قبل قنوات وشبكات الرقابة التابعة للدولة.

ولكن، يجب القول أن هذا الأمر لا ينفع إذا ما تدخلت الدولة أو العدالة، ففي سنة 2013، قام مكتب التحقيقات الفدرالي بإغلاق موقع طريق الحرير (Silk road) الذي كان موجود في الشبكة العميقة، وذلك بسبب أنه كان يوفر ويبيع المخدرات ، والمهلوسات، والأسلحة بطريقة غير قانونية، ولكن مثل الوحش الأسطوري *هايدرا أو عدار (Hydra)، ظهرت نسخة جديدة للموقع بعد شهر من إغلاقه، ولم يتمكن مكتب التحقيقات الفدرالي من تعقب الموقع حتى بعد سنة كاملة، وهذه الحالة تمثل نموذج للعديد من الحالات التي حصلت، الأمر الذي يوحي أنه لا فائدة من القيام بذلك.[21] وقد ذهب **سانجيرو كواباتاكي** (Pseudonym - Sanjuro Kuwabatake) ابعد من ذلك حين صرح سنة 2013، عندما أطلق موقع خاص بالقتلة المأجورين حيث اعتبر أن ذلك حتمية حين قال:[22]

---

[21] Michael Chertoff, Tobby Simon, **The Impact of the Dark Web on Internet Governance and Cyber Security** (Canada: Waterloo, Global Commission on Internet Governance, published by the Centre for International Governance Innovation and the Royal Institute for International Affairs, 2015) , P. 3.

[22] James Bartlet, ***The Dark Net, Inside the Digital Underworld*** (United Kingdom: London, published by William Heinemann, the first edition, 2014), P. 30.

"ومع ذلك، يمثل ما نقوم به اتجاه وتحول لا بد منه في ظل التطور التكنولوجي الذي نراه اليوم. . . فعندما يستخدم شخص ما القانون ضدك، أو ينتهك ويتعدى على حقوقك في العيش، وحقك في الحرية، والملكية، والكسب، والبحث على السعادة، ربما عليك الآن، وبطريقة آمنة كتواجدك في غرفتك، أن تحرص على تخفيض متوسط العمر الذي سيعيشونه في المقابل".

منا هنا تكون قد تكونت للدينا نظرة حول الشبكة العميقة، ونكون قد عرفنا أنها كما يقول البعض، بمثابة عالم سفلي حقيقي (Underworld)، يمكن أن تجد فيه أي شيء. ولكن بعيدا عن هذا الطرح، يقسم العديد من الخبراء، ومستخدمي الشبكة العميقة، هذا الجانب من الأنترنت إلى عدة أقسام، ومراحل، كل مرحلة لها ميزات مختلفة ومضمون محدد، والوسائل التي يتم استخدامها للنزول أو الصعود في هذه المستويات تعد مختلفة أيضا؛ لقد طرحت هناك العديد من التقسيمات، هناك من عرض 5 مستويات، وهناك من عرض أكثر من ذلك، لكن حاليا، المتداول، هي ثمانية مستويات التي اتفق عليها المجتمع الإلكتروني.

ووفق ما سبق يمكننا تقسيم الشبكة العميقة إلى عدة مستويات، مرتبة من حيث سهولة الولوج إليها وتوفرها، ويمكن التعبير عنها وفقا لما يلي:

1- في الأول، لدينا ثلاثة مستويات تعد بمثابة سطح الشبكة، وفي هذه المستويات يكمن معظم المحتوي الذي يمكن الدول إليه بالوسائل التقليدية، كما أن فهرسة محركات البحث فاعلة في هذه المستويات، لكن يجب ذكر أنه هناك تواصل بين المستوى الثالث والرابع، وذلك بسبب قدرة الأشخاص على الولوج إلى بعض محتوى المستوى الرابع عبر التحميل الغير قانوني للملفات عبر استخدام العديد من البرامج أو الملفات ذات الامتداد (Torrent.) ، كما أن الولوج إلى هذه الملفات انطلاقا من هذه المستويات، يمكن يعرض صاحبه بشكل كبير للخطر، ذلك أن معظم المواقع، وشركات الاستضافة والتحميل، وموفري الخدمة الشبكية، تحت رقابة كبيرة، لديها قوانين صارمة حول الملكية الفكرية.[23]

[23] Bin He, Mitesh Patel, Zhen Zhang, Kevin Chen, Chuan Chang, "Accessing the Deep Web: A Survey," in **Communications of the ACM**, No 5, volume 50, (may, 2007), pp. 95-101.

2- المستوى الرابع، وهو تعبيرا آخر على استعمال البرامج الخاصة للدخول الشبكة العميقة، إذا لا يمكن الإبحار في هذا المستوى وبقية المستويات إلا عند استعمال برامج خاصة مثل تور، ومعظم المحتوي
3- الذي يمكن الولوج إليه بسهولة في الشبكة العميقة موجود في هذا المستوى، ونقصد هنا بمعظم المحتوى؛ أي محتوى لا يحتاج إلى إمكانيات فيزيائية إضافية من أجل الولوج إلى محتوى معين، أي أن امتلاك برنامج تور فقط كفيل بتصفح المحتوى البصلي (Onion).
4- المستوى السادس، والسابع، ويطلق البعض على هذه المستويات اسم حساء الفيروس (Virus Soup)، وفي هذه المستويات تكمن حوالي 80% من بيانات الشبكة العالمية، لكن الدخول إليها يحتاج إلى خوارزميات كمية معقدة (Polymeric Falcighol Derivation)، وأنظمة الحماية المغلقة (Closed Shell System). [24]
5- المستوى الثامن، والذي يطلق عليه اسم الزعيم الأخير (The Final Boss) من قبل المجتمع الإلكتروني، أو النظام الأولي أو المسيطر (The Primarch System)؛ وهذا المستوى يشير إلى السيطرة التامة على الشبكة، خاصة المفاتيح الكمية للولوج إلى كامل الشبكة، ولكن حاليا لا توجد تكنولوجية قوية بشكل كافي من اجل كسر الحماية والحصول على الخوارزمية النهاية، فحاليا حتى أبسط التشفير (2048-bitRSA) الذي يتم اعتماده من قبل برامج الفدية الإلكترونية (Ransomware)، لا يمكن تكسيرها إلا بعد قرون وفقا للقدرة الحاسوبية الحالية.[25]

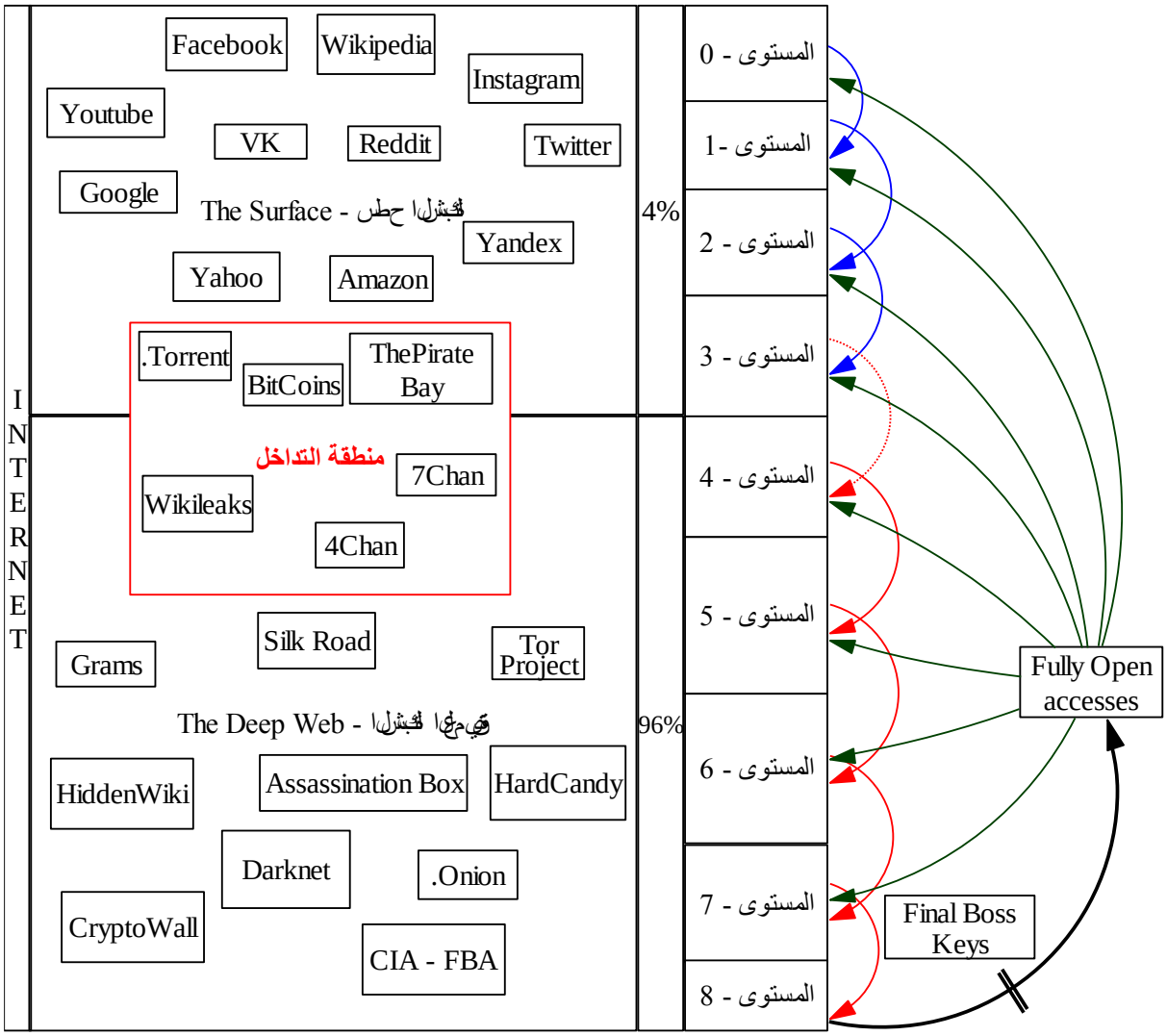
ولكن يجب الذكر هنا أنه لا يوجد هناك اتفاق حول عدد أو شكل هذه المستويات، مع أن الجميع يتفق على وجودها. فالعالم الإلكتروني عكس العالم المعاش، هو مجال لا أحد يمكن السيطرة عليه بشكل كامل، وعكس العديد من المراكز البحثية والأكاديمية، يساهم في هذا العالم كل شخص لديه القدرة في ذلك، ففي ظل المعرفة التي أصبحت مفتوحة للجميع، وتوفر الخصوصية في الشبكة العميقة، برزت هناك العديدة من النماذج التي قدمت برهانا حول لامركزية الإنتاج والإبداع في العالم الشبكي.

---

[24] Anonymous Hacktivism,"DeepWeb Infography," in: **https://goo.gl/jAQgYR**,(Wednesday, April 27, 2016).

[25] المكان نفسه.

الجدول رقم: 1.0



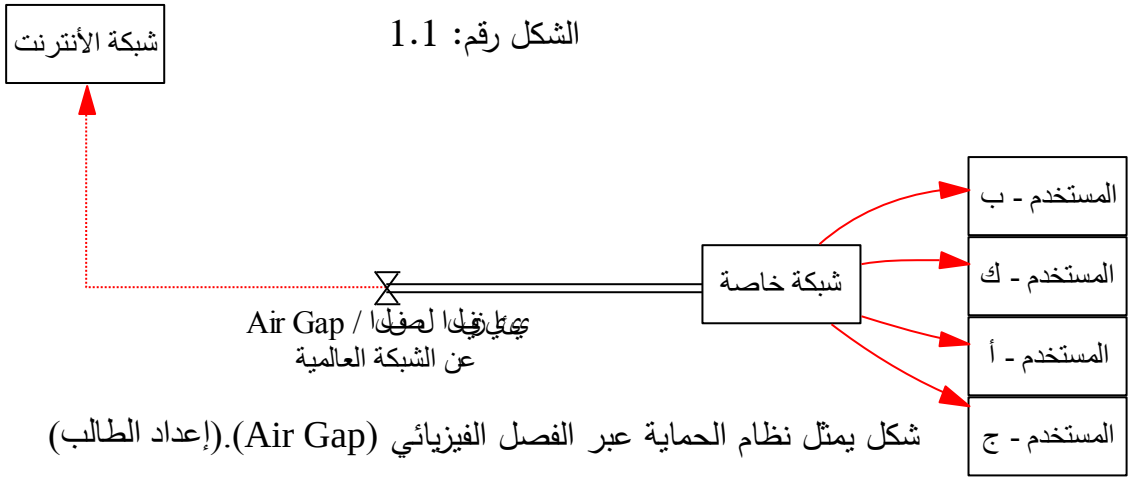
جدول يمثل وصفا هيكليا للشبكة، والمستويات التي يمكن الولوج إليها.

أكانت الجريمة مرتفعة بشكل فائق أو لا، أكان الأمر قانوني أو لا؛ علينا أ نقر بأن الشبكة العميقة، رغم خطورتها وما يوجد فيها، تعد أحد مقومات الأنترنت الذي نعرفه اليوم، وبفكرة أخرى، أصبح هناك عالم موازي ينشط فيه الأشخاص، عالم تتقاتل فيه المصالح السياسية والاقتصادية لدول العالم في الخفاء، فمثل ما هو الحال مع أنونيموس (Anonymous) التي تعمل في النضال والمقاومة عبر الاختراق، وإرسال الرسائل، وتسريب المعلومات، والتسبب بأضرار اقتصادية، تعد الشبكة العميقة الآن معقل ذو وجهة متزايدة، واي جهة ، تريد السرية، أو الإتلاف، أو تحقيق الفائدة، أو الضرر، عليها النزول إلى عالم الأنترنت السفلي، ففي ظل تزايد محركات البحث في الشبكة العميقة، كما عمليات الفهرسة، سيصبح الإبحار فيها قريبا، أمرا روتينيا ومتاحا أكثر.

1.2.1 فجوة الهواء

إذا قلنا من قبل أن الأنترنت هي مجموعة من الشبكات المرتبطة ببعضها البعض على الصعيد العالمي، فالشبكات المفصولة فيزيائيا وهيكليا (Air-Gapeed/Air-Gap Networks)، هي شبكات معزولة ومفصولة من الناحية الأنظمة، ومن الناحية الفيزيائية من الشبكات العامة، أي الشبكات التي يمكن للعامة الوصول إليها مثل ما هو الحال مع شبكة الأنترنت العالمية، كم من ناحية أخرى، هذه الشبكات أيضا مفصولة هيكليا من ناحية الربط الداخلي للشبكة في حد ذاتها.[26] والتكلم على هذه نوع من الدفاع الإلكتروني يعد جد مهم في مجال العلاقات الدولية، خاصة وأنه هناك العديد من الدول التي اعتمدت على هذه الطريقة من أجل حماية أمنها الخاص من التجسس الصناعي، ومن الهجمات الموجهة لتمدير البنى التحتية، أو حتى التحكم في المعلومات التي تأتي من الخارج، أو التي تخرج من الداخل.

الشكل رقم: 1.1



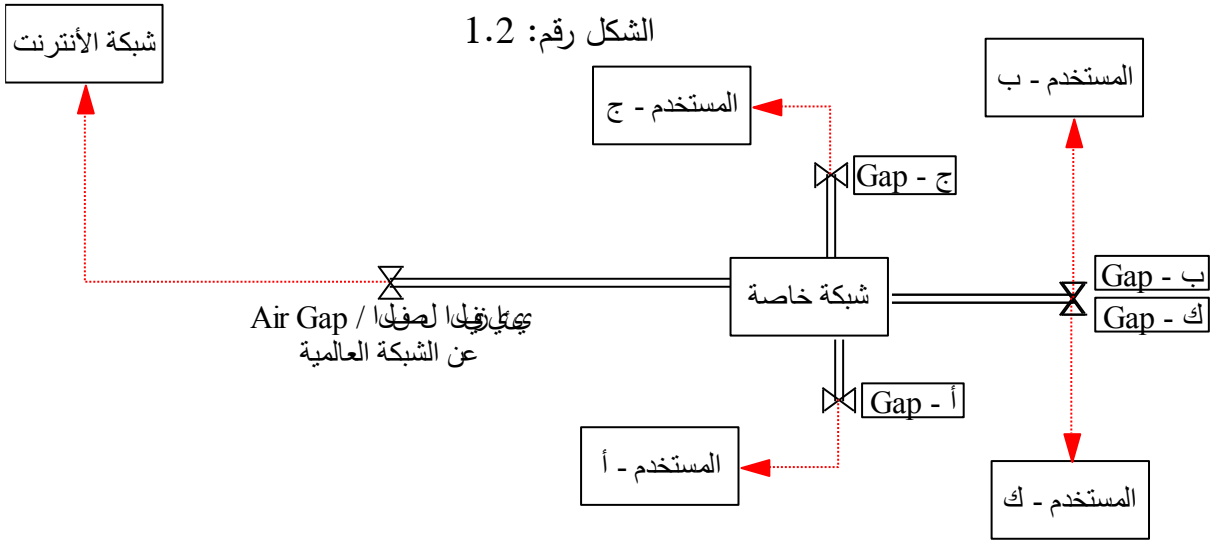
شكل يمثل نظام الحماية عبر الفصل الفيزيائي (Air Gap).(إعداد الطالب)

وربما يعد الأمر في بعض الأحيان، حتمية ضرورية، مثل ما هو الحال عندما أعلن المرشد الأعلى الإيراني علي خامنئي سنة 2012، إلى ضرورة إقامة شبكة داخلية مفصولة كليا على الشبكة العالمية، وذلك من أجل الحفاظ على المضمون والثقافة الإسلامية، والأهم من ذلك، هو الحفاظ على أمن البلاد من الهجمات الإلكترونية العديدة التي تتعرض إليها؛ ولهذا ومنذ هذا الإعلان، تعمل إيران على إقامة هيئة مركزية داخل البلاد من أجل التحكم في تدفق المعلومات، أو فصل الاتصال مع الشبكة العالمية إذا

(26) Mordechai Guri, Assaf Lachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, Yval Elovici, **GSMem : Data Exfiltration from Air-Ga pped Computers over GSM Frequencies** (Negev: Published by Ben-Gurion University, the first edition, 2015), p.849.

اقتضت الحاجة ذلك، [27] ولكن هذه العملية والتفاؤل لا يتقاسمه الجميع، خاصة الدول الكبرى، مثل الولايات المتحدة الأمريكية، والمنظمات الحقوقية التي ترى في مثل هذه المبادرة، كخرق لحقوق الإنسان في حرية التعبير، وفي وصوله للمعلومات. وفي الشكل التالي يمكن رؤية النوع الثاني من نظام الحماية عبر الفصل والذي في هذه الحالة يعتمد على آلية الفصل الهيكلي حتى داخل الشبكة المغلقة، وفي العادة تكون عبارة عن بروتوكولات يتم اعتمادها لمنع انتشار الخطر، وهذا النموذج يمكن تطبيقه داخل المؤسسات والمنظمات، أو على سلم أوسع.

الشكل رقم: 1.2



شكل يوضح، ألية الفصل الفيزيائي، مع إدماج هيكلي داخل الشبكة المغلقة، من أجل اقصى حماية ممكنة.

(من إعداد الطالب)

ويجب القول هنا، أنه وعلى مستوى العلاقات الدولية، لا تعد إيران الدولية الوحيدة التي قامت بمبادرات من أجل حماية، أو السيطرة على المعلومات المتدفقة على الشبكة، فقد قامت الصين بما تم تسميته لاحقا بـ جدار الصين الناري العظيم (Great Firewall of China)، [28] ويعد مشروع هذا الجدار جزء من مشروع أوسع اسمه مشروع الدرع الذهبي (Golden Shield Project)؛ فقد كانت هذه المشاريع موجهة خاصة من أجل الأمن الشبكي والحماية الإلكتروني، كما كانت أيضا موجهة من أجل التحكم، والحجب، والرقابة. لقد بدأت الصين في العمل على إعداد أرضية هذا المشروع بداية سنة

[27] Farnaz Fassihi, "Iran's Censors Tighten Grip," in: **http://goo.gl/3Htu80**, (Wednesday, April 27, 2016).

[28] Norris Pi ppa, ***World Bank Staff Public Sentinel: News Media and Governance Reform*** (The Unites States of America: Washington DC, Published by the World Bank, the first edition, 2010), p. 360.

1990،[29] وتم إطلاقه بكامل أنظمته وبشكل رسمي سنة 2003، [30]وقد اعتمد هذا النظام على العديد من طرق الحجب والتحكم والرقابة مثل ما هو الحال مع حجب العلب الإلكترونية للعديد من موفري الخدمة الذين لا يحترمون السياسات الصينية، وحجب الخدمات الوكيلة (Proxy)، وأسماء النطاقات (DNS)، وبروتوكولات الأنترنت (Internet Protocol - IP)، ويمكن القول هنا أن الطرق في تطور مستمر لتجدد الطرق التي يتم استخدامها للالتفاف على الحجب مثل ما هو حال مع شبكة *تور (Tor)، لهذا هناك تحديث مستمر وفعال لهذا النظام والمشروع من أجل مواكبة التقانة الحديثة.

فبعد الجو، والبحر، والأرض، والفضاء الخارجي، لم يكن أحد ليعرف أن العالم الافتراضي سيصبح هو الآخر احد مجالات التنافس الإنساني، ففي ظل عالم أصبح فيه الاتصال مع العالم الخارجي، أحد مقومات الاقتصاد القوي، والأمن، والتطور العسكري؛ أصبح من الواضح جدا بالنسبة للصين أنه عليها المرور قدما في تحديث نفسها في هذا المجال؛ رغم أن ذلك يعني من جانب آخر، الاستعداد وقبول هامش الخطر الذي يجلبه هذا النوع من التكنولوجيا أيضا. [31]

ولكن يجب القول أنه في الأخير، وحتى لو أن نظام الفجوة يعطي حماية كبيرة للأنظمة؛ كونه يعد أحد أنواع الشبكات المغلقة، إلى جانب شبكة الأنترنت والشبكة العميقة، إلا أنه في عصر التقانة، لا يجب أبدا أخذ أي شيء كمُسلمة، فمؤخرا تم عرض العديد من الطرق التي تعتمد على موجات الراديو التي تطلقها أجهزة الحاسوب من اجل سحب المعلومات، أي تحويل المركبات الداخلية للحاسوب إلى ما يشبه الهوائي، والذي يمكن التقاط إشاراته الكهرومغناطيسية عن بعد عن طريق أي هاتف أو جهاز خاص،[32] فعند تنقل المعلومات بين المعالج والذاكرة الحية، يقوم الحاسوب إصدار موجات راديو وصوتية قوتها بين

---

[29] Greg Walton , ***China's Golden Shield: Corporation and the Devlopement Surveillance Technology in the People's Republic of China*** (Canada: Montreal, published by The International Centre for Human Rights and Democratic Development,2001.), p. 11.

[30] Xiao Qiang, "How China's Internet Police Control Speech on the Interne," in: **http://goo.gl/OlKtbx**, (Wednesday, April 27, 2016).

[31] Daniel Ventre , ***Chinese Cybersecurity and Defense*** (The United States of America: Hobken, Published by Joan Wiley & Sons Inc, the first edition, 2014), pp. 11-26.

- تور (Tor) : متصفح يقوم على التسيير البصلي اللامركزي (Onion routing)، تم تطويره في التسعينات من قبل وكالة مشاريع البحوث المتطورة الدفاعية (Defense Advanced Research Projects Agency)، ومعمل أبحاث البحرية الأمريكية، من اجل تبادل المعلومات بسرية، أخرج للاستخدام العام سنة 2006.

[32] National Aeronautics and Space Administration, Under the Foia case 51633, Tempest: A Signal Problem, the story of the discovery of various compromising radiation from communication and Comsec equipment, spectrum cryptologic field, 2007. pp. 1-2.

0.1 و0.15 ديسيبال (Decibel) يمكن إلتقاطها عن بعد، وتحويلها إلى بيانات حاسوبية عبر برامج متخصصة، من أجل الإطلاع عليها، الأمر الذي يشير إلى صعوبة فعلية في تحقيق أمن فعلي إذا ما تعلق الأمور بالموارد الإلكترونية.

1.3 الأمن

يعد الأمن مفهوما واسعا، من حيث المضمون، ومن حيث الاعتبار التقديري لما يصب في دائرة الأمن، فالأمن يمكن أن يكون، يتعلق بالغذاء، والشعور الذاتي بالأمان، والقدرة على القيام بعدة وظائف بطريقة عفوية وديناميكية، كما يمكن أن تكون له علاقة بمميزات فيزيائية بحتة، لا علاقة لها بالإنسان، فما يعد شيء لا علاقة بالأمن، يمكن أن يمثل في جهة أخرى محددا للأمن أيضا؛ هذه الصفات الزئبقية للأمن جعلت منه مفهوما واسعا جدا لا يمكن تحديده بطريقة سهلة، وأفضل طريقة للتعاطي مع مفهوم الأمن، هي محاولة فهمه من خلال التعاطي مع كل حقل على حدى، وذلك من أجل فهم طبيعة ومحددات الأمن في ذلك المجال، فلمدة طويلة، كان الأمن والأشياء أو المركبات الصغيرة التي تعبره عنه ويقوم عليها، خاضعة للتقدير الإنساني، أو أن مفهوم الأمن يعبر عن ذهنية لها علاقة بوجود الشخص وتحقق مصالحه على أي مستوى ممكن، فأمان منطقة معينة، أو طاولة معينة، أو محصول معين، يُربط للتأثيرات السلبية التي يمكنها أن تحصل للإنسان، لهذا وضع الإنسان في المركز، فيما يخص القضايا الأمنية؛ طبعا هذا كان قبل أن تحدث العديد من التحولات في مفهوم الأمن، أو تقدير الأمن، من اعتبار الإنسان كمركز، إلى التعامل بمعادلات أكثر شمولية، تشمل الدورة الطبيعية، في شقها المادي، والمعنوي.

ولهذا ففي دراسة هذا الموضوع، فمن الواضح جدا أن محاولة فهم الأمن الإلكتروني، وموضعه من المعادلة الدولية الحالية، يؤدي بنا إلى محاولة فهم، الدور الذي يلعبه الأمن، والذي يعد بمثابة الحاقِن للعديد من السياسات، والعلاقات بين المجتمعات، والدول، وكل مكونات المجتمع العالمي حاليا، كذلك وكما عبر كل من البحاث **باري بوزن** (Barry Buzan) ، والباحثة **لين هانسن** (Lene Hansen) حين أكدا على أنه :[33]

[33] Barry Buzan, Lene Hansen, **The evolution of International Security Studies** (The United States of America: New York, published by Cambridge University Press, the first edition, 2009), pp. 22-23.

"يستحيل فهم كل النقاش الذي يدور حول الدراسات الأمنية في العلاقات الدولية، وكيفية تطورها، بدون أن تتوفر بعض المفاتيح حول الموضوع... كما أن التحولات التي حصلت في هذا الموضوع، من القرون الوسطى إلى الشكل الحالي للنظام، كانت كبيرة جدا".

فقد نفهم من الذي طُرح هنا، على أن قضية الأمن لا تعد قضية منفردة في حد ذاتها، بل كانت في العديد من الأحيان، تتعلق بالعديد من القضايا على مر التاريخ، فالأمن كمفهوم، أو كسلوك، ينظم ويضبط القرارات الإنسانية منذ عصور، جعل منه أحد المحددات، أو أكبر مؤثر على الحياة السياسية، خاصة في القضايا التي كانت تتعلق بالدولة الحديثة، والسيادة، والملكية، الأمر الذي جعل من الأمن، أو الدراسات الأمنية، لها علاقة وطيدة بالعلاقات الدولية:[34]

"رغم أنه هناك تساؤل مفاهيمي، حول أين تنتهي الدراسات الأمنية، وأين تبدأ العلاقات الدولية، من حيث الدراسة، فالحدود بين الدراسات الأمنية، والعلاقات الدولية، يصعب رسمها، فمنذ مدة، وخاصة بعد الحرب العالمية الثانية، كان الجواب على هذا السؤال، على الفرق بين الدراسات الأمنية، والعلاقات الدولية، يمكن في أن الدراسات الأمنية، تركز على استعمال القوة في العلاقات الدولية."

فإذا راينا الأمن من زاوية الدراسات الأمنية، خاصة منها التي لها علاقة بالعلاقات الدولية، يمكننا أن نجد العديد من الطروحات التي حاولت فهم الأمن، كما حاولت إيجاد الطريقة المثلى لتوظيفه في تسيير السياسة الخارجية أو الداخلية للدولة، فمن بين هذه النظريات يمكننا أن نجد، الواقعية ، والواقعية الجديدة، الليبرالية، والليبرالية الجديدة، البنائية، الماركسية، النسوية، السلام الأخضر، الوظيفية؛ كل هذه النظريات عالجت مسألة الأمن، وحاولت أن تعطي النموذج الأنجع بنظرها، لفهم مختلف التفاعلات التي تحدث على المستوى الدولي، من اتجاهات كانت تتكلم على محورية الدولة وعسكرية القوة والأمن، إلى تحول جديد أوسع، فرضته التحولات الدولية، نحو أمن إنساني الذي يركز أكثر على المخاطر الجديد والمتزايدة والتي لا يمكن حلها إلا بالتكاتف عبر التركيز أكثر على الإنسان والمخاطر المشتركة التي يعاني منها،[35] فالنظرة إلى الأمن كمفهوم على يركز فقك على القوة العسكرية لا يعد جديدا، إذ يمكننا

---

(34) **Ibid**, p.16.

(35) Christopher P.M Water: British and Canadian Perspectives on international Law, (The Netherlands, Leiden, published by Martinus Nijhoff, the first edition, 2006), p.210.

أن نجدها حتى في إسهامات الاستراتيجي العسكري الصيني **صن تزو** (Sun Tzu 544 BC- 496 BC)، حين أشار إلى أهمية الاهتمام بالجانب الأمني الذي لا يتعلق بالحرب، وذلك عبر الاهتمام بالموارد وكيفية التعامل بها انطلاقا من مبدأ الاستدامة، وتكلمه على الأمن الفكري، والروحي، والمعنوي للشخص.[36]

ففي هذه المحاولة من أجل فهم الدور الذي أصبح يلعبه الأمن الإلكتروني في مكافحة الهيمنة في العلاقات الدولية، يجب أن نتعامل مع القضية من منطلق دقيق وشامل، كون الأمن في عصر الرقمنة، لم يعد يمتاز بتلك المركزية التي جاءت بها الدولة الحديثة، فالتعامل أصبح بشكل أكبر يخضع للمتغيرات الفردية، بعيدا عن كل محاولة نظرية، كنوع من التحرر، والعودة إلى الوراء.

فمثلا، نجد أن عالم النفس الأمريكي، **أبراهام ماسلو** (Abraham Maslow 1908-1970)، يعالج مسألة الأمن في كتاب الدوافع والشخصية (Motivation and Personality)، والذي نشر سنة 1954، حيث يقول:[37]

> "**إذا تم تحقيق الرغبات الفيزيولوجية بشكل كافي، عندها ستظهر حاجات جديدة، والتي يمكن أن نطلق عليها اسم الحاجة إلى الأمان (الأمن، الاستقرار، الحماية، التحرر من الخوف، والقلق، والفوضى، والحاجة إلى التنظيم، الهيكلية، القانون، الحدود، القوة في الحامي، إلى غير ذلك)**".

يمكننا أن نرى هنا تشابه في الطرح الذي قدم **ماسلو**، مع رؤية **باري بوزن** الذي يرى على أن الأمن هو عملية تهدف إلى التحرر من التهديد، [38] ويتكلم **أرنولد والفر**(Arnold Wolfers 1892-1968) في نفس السياق حين يقول أن الأمن يعبر عن الحالة التي يغيب فيها الشعور بالخطر، والخوف، وتكلم عن احتمال العلاقة بين القوة والأمن، خاصة إذا كان الأمن لا يتوفر إلا عند وجود تراكم مستمر

---

[36] Luo Zhiye, ***Sun Tzu's, The Art of War***(China: Beijing, published by The Foreign Translation Publishing House - The State Administration of Press, Publication, Radio, Film and Television of the People's Republic of China, 2007), p. 17-22.

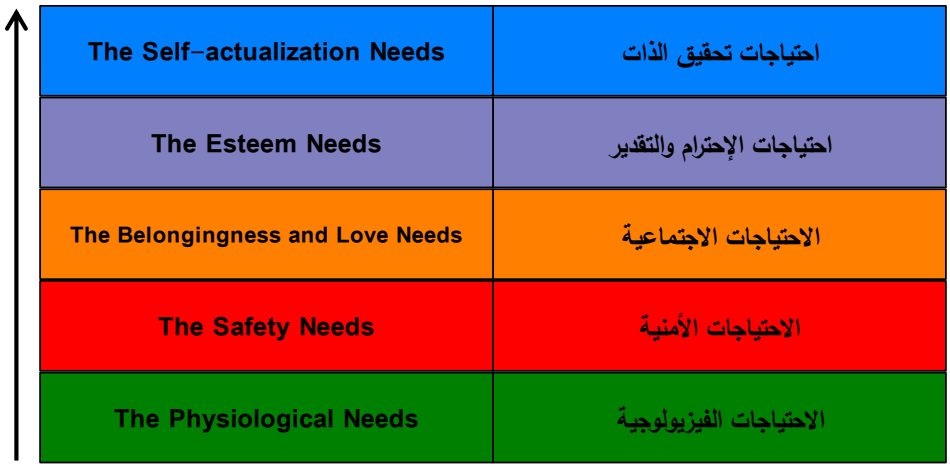
[37] Abraham H. Maslow, ***Motivation and Personality*** (The United States of America: Cambridge, published by Harper & Row, the third edition, 1954), p, 18.

[38] Barry Buzan , ***People State And Fear , An Agenda For International Security Studies In The Post-Cold War*** (The United States of America, Bonlder published by Lynne Rienner Publishers ,the first edition, 1991). P. 18.

للقوة،[39] وأضاف المحلل، والمنظر في العلاقات الدولية **جوزيف ناي** (Joseph Samuel Nye) بعدا آخر في تعريفه للقوة حين قال:[40]

"يمكن اعتبار القوة مثل الأحوال الجوية، فالجميع يتكلم عليها، لكن القليل فقط يفهمها، فمثل ما يحاول الفلاحون، وعلماء الأرصاد الجوية فهم والتنبؤ بأحوال الطقس، يحاول في الجانب الآخر القادة السياسيين، والمحللين، فهم وتحليل علاقات القوة، والتنبؤ بالتحولات التي يمكن أن تحصل. والقوة أيضا مثل الحب، يسهل التعايش في حضنه، لكن يصعب تعريفه أو قياسه. "

الجدول رقم: 1.1



ترتيب الحاجيات الإنسانية، وفق طرح أبراهام ماسلو.[41]

الأمر المهم هنا، وخاصة إذا ما ربطنا الأمر بما أحدثه الأمن الإلكتروني في العلاقات الدولية، عبر تجديد العودة إلى النظام البدائي لتوزيع القوة، فقد عبر **ميرشايمر** في موضوعه حول الواقعية البنائية، على ما اسماه: مُنظورا الواقعية البدائية، الذي كانوا يروا، ومن بينهم **هانس مورغنثو**(Hans Morgenthau 1904-1980)، أن الإنسان لديه طبيعة شريرة، وهو في سعي دائم من اجل امتلاك القوة

[39]Arnold Wolfers, "National Security as an Ambiguous Symbol," in ***Political Science Quarterly***, No 4, Volume 67(December, 1952), pp, 481-502.
[40] Joseph Samuel Nye , ***Soft Power, The Means to Success in World Politics*** (The Unites States of America: New York, published by PublicAffairs™, the first edition, 2004.), p, 1.
[41] ***Ibid***.

والسيطرة؛[42] فإذا عالجنا هذه الفكرة في نفس السياق التي تدعوا إليها نظرية العقد الاجتماعي عند كل من **توماس هوبز**(Tomas Hobbes 1588-1679)، و**جون لوك**(John Locke 1632-1704)، و**جان جاك روسو**(Jean Jacques Rousseau 1712-1778)، سنجد أن القوة ، والأمن، لهما دورا مهما في هيكلة النظام الاجتماعي، والذي في الغالب يتعلق باحتكار القوة، وتحقيق الأمن.

لكن حاليا، لم يصبح بمقدور الدولة احتكار القوة بشكل كامل، ففي ظل الرقمنة، والاعتماد المتزايد على التكنولوجيا، أصبح بإمكان أي شخص أن يسبب أضرار تتعدى أضرار عدة حروب مجتمعة، ويمكننا أن نرى هنا، نوع من التحرر، نوع من العودة إلى الوراء، إلى مرحلة ما قبل العقد الاجتماعي، المرحلة التي كان بإمكان أي شخص أن يصنع سلاح، أو أي شيء ليلحق به الضرر. ومما لا شك فيه ، وفيما يخص الأمن الإلكتروني، فوتيرة المخاطر الإلكترونية ستزداد أكثر، فكلما أصبحت المعرفة مفتوحة أكثر، وكلما اتجهنا أكثر نحو رقمنة حياتنا؛ كلما أصبحت القوة موزعة وغير مركزية.

من جانب آخر، هناك من يتكلم على الأمن من منطلق القوة كما قال **والفر**، أي بموضوع إجبارية، أو ضرورية استعمال القوة في أي إجراء ،أو وضع معين يتعلق بالأمن؛ ذلك أن القوة دائما ما تكون مفهوما ملازما للأمن، سواء كان ذلك من أجل تحقيق الصالح العام لتجنب أخطار محتملة، أو من أجل تحقيق مصالح معينة، ومحددة، على حساب أي شيء آخر، فهذا الطرح ينظر إلى القوة كمفهوم أكثر توسع، كأن ينظر إلى أن توفر الأمن في موضع معين، يحتاج إلى قوة ذهنية تقدر معنى الأمن، الأمر الذي يشير هنا، إلى زئبقية كبيرة في التعامل مع هذه المفاهيم.

يرى **ناي**، أن تطور مفهوم القوة يمكن التعبير عليه بما يسمى حاليا: بالأوجه الثلاثة للقوة (The Three Faces of Power)؛ فالوجه الأول تم التعبير عليه من قبل **روبرت ألان دال** (Robert Alan Dahl 1915-2014)، والذي يرمي إلى أن القوة هي إجبار جهة معينة على القيام بشيء ما كانت لتقوم به لولا استعمال القوة، وفي سنة 1960 عبر علماء السياسة على أن نظرة روبرت إلى القوة، تفتقد إلى الوجه الثاني للقوة؛[43] فقد تم التعبير على الوجه الثاني للقوة سنة 1970، من قبل المنظر في علم الاجتماع ، والسياسة **ستيفن لوك** (Steven Luck) لما تكلم على الأجندات، حيث يرى **ستيفن** أن

---

[42] جون ميرشايمر، الواقعية البنيوية، شريط مصور، في: **https://youtu.be/gh6bYUsJY6g**، السبت، 30 نيسان، 2016.

[43] Joseph Samuel Nye, ***Cyber Power*** (The United States of America: Massachusetts, published by Belfer Center for Science and International Affairs, essay from The Future of Power in the 21st Century, 2010.), p. 2.

الشخص الذي يضع الأجندة هو الشخص الذي يمتلك القوة، وهذه الصورة يمكن فهمها مثلا عندما يخاطب الرئيس بقية العاملين في اجتماع معين، فهو لديه القوة، ولو تحداه أحد يمكنه أن يغير طبيعة الحديث؛ يشار هنا إلى أن **ستيفن** وضع أيضا 3 مستويات لدراسة القوة، عبر فيها عن مرورها من الإكراه، إلى الأجندة، إلى الإقناع السالب الذي يعتمد في طريقة تجسيده على القوة الناعمة.[44]

فقد أضاف **ناي** بعد طرحه للوجه الثاني للقوة، إضافته التي جاء بها سنة 1990، والتي تتعلق بالقوة الناعمة، والتي برأيه فرضتها المستجدات الدولية التي جعلت دول مثل الولايات المتحدة الأمريكية، تتقاسم دورها القيادي، مع فواعل جديدة في المجتمع الدولي، فالأمن الإلكتروني، والسعي إلى الهيمنة الإلكترونية، يشكل أحد التهديدات التي يصعب السيطرة عليها، خاصة بسبب أننا على أبواب عصر ستتراجع فيه الجغرافيا التقليدية إلى مفهوم هجين، وجديد، يعبر عن السيادة، [45] وقد عرف **ناي** القوة الناعمة على أنها:[46]

> "**القدرة على التأثير في خيارات الآخرين على المستوى الشخصي، فجميعنا على دراية بقوة الجذب، والرغبة ... فالقوة تكمن في تلك الكيميائية الغامضة التي تقوم بالجذب، ففي عالم الاقتصاد يعلم القادة جيدا، أن الأمر لا يتعلق فقط بإعطاء الأوامر، بل بالاعتماد أيضا على جذب الآخرين بطريقة تجعلهم يقومون بالعمل**".

وقد أضاف **ناي** تعريفا آخر للقوة، ولكن في السياق الذي يتعلق بالأمن الإلكتروني، أو الفضاء الإلكتروني؛ يرى **ناي** أن القوة الافتراضية (Cyber Power)، هي القوة التي تستند على المعلومات، ونعني بذلك، كل الموارد التي لها علاقة بالتحكم في الاتصالات، والإلكترونيات، والحواسيب، والشبكات، كما أيضا القدرة على التحكم في التقانة الخلوية، وأنظمة الاتصال الفضائية. ووفق ما سبق يمكن تعريف القوة الافتراضية على أنها:[47]

> "**القدرة على استخدام الفضاء الإلكتروني، من اجل خلق تفوق، والتأثير على الأحداث، عبر مختلف البيئات التشغيلية، وأدوات القوة.**"

---

(44) Keith Dowding: "Three-Dimensional Power: A Discussion of Steven Lukes' Power: A Radical View", in ***Political Studies Review***, No 2, Volume 4(February 2006), pp, 136-145.
(45) Joseph Samuel Nye, Cyber Power, ***op. cit***, pp. 2-3.
(46) Joseph Samuel Nye, Soft Power, ***op. cit***, p. 5.
(47) Joseph Samuel Nye, Cyber Power, ***op. cit***, pp. 4-3.

الجدول رقم: 1.2

الوجه الأول للقوة – 0591	Robert Alan Dahl
إجبار "أ" على القيام بـ "ج"، بحيث أن "أ" لن تقوم بـ "ج"، إلا عند إستخدام القوة ضدها	
الوجه الثاني للقوة – 0791	Steven Luck
الجهة التي تضع الأجندة، و تحدد قوانين اللعبة الحالية، هي التي تمتلك القوة	
الوجه الثالث للقوة – 0991	Joseph Samuel Nye
القوة الصلبة، والقوة الناعمة؛ بين الإكراه، و وضع الأجندات	

جدول يوضح الأوجه الثلاثة للقوة وفقا لناي. (من إعداد الطالب)

في الأخير يمكننا أن نرى هنا أن مفهوم القوة، والأمن، أطر بشكل كبير من أجل فهم السلوك التقليدي للدول، كم التفكير التقليدي الذي ساد في العلاقات الدولية، فالتكلم على العلاقات الدولية، في ظل التطور التكنولوجي، أصبح يأخذ حيزا اكبر في النقاش الذي يدور الآن في الساحة الدولية، فالأمن الإلكتروني، كأسلوب جديد لمكافحة الهيمنة، لم يتم إدراجه في كل الأنظمة المعمول بها في العلاقات الدولية، إذ يمكننا أن نجد حاليا العديد من الثغرات، مثل ما هو الحال مثلا مع موضع الأسلحة الإلكترونية من بروتوكولات جينيف، كما التقانة من الدراسات الأمنية، والنظرية في العلاقات الدولية؛ لكن الذي يمكن قوله هنا، هو أنه لو حاولنا فهم ما يمثل الأمن الإلكتروني، من منظور الأفكار السائدة حاليا في مجال التنظير في العلاقات الدولية، سنجد هناك صعوبة كبيرة من الناحية المنهجية، حتى لو كانت هناك أفكار عامة وأساسية يمكن اعتماده من أجل فهم هذه الموجة الجديدة.

1.3.0 الأمن الإلكتروني

يمثل الأمن الإلكتروني مفهوما مركبا، يشمل العديد من الإجراءات الأمنية، وأنواع المخاطر التي لها علاقة مباشرة بالإلكترونيات وتنقل البيانات وتأمينها، كما أيضا لها علاقة بأي نظام أو دائرة إلكترونية يمكن استغلالها من أجل تحقيق منفعة معينة أو إلحاق الضرر لأي أغراض معينة، فالتكلم على ما هو إلكتروني يوصلنا إلى اعتبار الأمن الإلكتروني ينطبق على صعيد الحماية الإلكترونية للأنظمة الفيزيائية (Hardware) والتي تمثل كافة المعدات الملموسة مثل المعالج (Central Processing Unit)، أو لوحة النظام (System Board)، أو أية معدات يمكن التعامل معها مباشرة ويمكن أن تتراوح بين معدات بسيطة متاحة للعامة، إلى هياكل تابعة للشركات الكبرى والحكومات.

ومن جانب آخر لدينا البرمجيات (Software) المعتمدة لتشغيل الأنظمة وتحديد طريقة عملها، فالبرمجيات هي بمثابة المُصَرف (Compiler) للأوامر كي يستطيع الحاسوب قرأتها، كون الحاسوب أو أنظمة الحاسوب الفيزيائية يمكنها فقط فهم نظام العد الثنائي (Binary Numeral System) ; والذي يعتمد على وحدة البِيت أو البايت (Bit) ،[48] أي 1 و0، ولهذا وفي نظرية المعلومات (Information Theory) يمكن القول أن البيت يمثل أقل قيمة ممكنة من المعلومات، يمكن نقلها في المجال الإلكتروني، فالبيت يعد وحدة قياس واللغة الوحيدة التي يفهمها الحاسوب، والمُصَرفات هي البرامج التي يعتمدها المبرمجون، من أجل تحويل أموار مكتوبة بشكل عادي، إلى أوامر يمكن للحاسوب قرأتها وفهمها، حتى أن المحقل أو الترانزستور ،ومنذ اختراعه وإلى حد الآن لا يعالج إلا حزمة المعلومات المتتالية والمكونة من الرقمين 1 و0.

فالأمن الإلكتروني، يعكس الوسائل المادية، والتي يمكن التعامل معها بطريقة مباشرة، مثل ما هو الحال مع الأسلحة؛ له لغة خاصة، وعالمية يتعامل بها، وهذه اللغة العالمية تمثل الحجر الأساس حاليا للفضاء الإلكتروني الحالي، فالشيء الذي يميز السلاح الإلكتروني، عن السلاح العادي، هو تعامله مع تفاعلات فيزيائية ما دون ذرية(Subatomic)، فمن أجل فهم

---

(48) Torben Aegidius Mogensen , ***Basics Of Compiler Design*** (Denmark: Copenhagen, University of Copenhagen, published by the Department of Computer Science, the 10 years edition, 2010.), pp. 1-2.

الأمـن الإلكترونـي، يجـب أولا معرفـة كيفيـة عمـل هـذا العـالم الافتراضـي، والحـدود التـي يمكنـه الوصـول إليهـا، وخاصـة وأن العـالم الإلكترونـي فـي تطـور مسـتمر نحـو الحواسـيب الكميـة(Quantum Computers) الفائقـة القـدرة،[49] هـذه الحواسـيب الكميـة ستسـتعمل الكوبيـت (Qubit) بـدل البييـت، وسـتكون لـديها قـدر أكبـر فـي تحليـل المعلومـات والحسـابات، كمـا ستحسـن بشكل أكبر الخصوصية والحفاظ على المعلومات.[50]

ومما يلي يمكننا أن نرى نموذج بسيط لمجموعة من الكلمات التي تم تحويلها من اللغة العادية إلى لغة نظام العد الثنائي:

> "Two possibilities exist: either we are alone in the Universe or we are not. Both are equally terrifying."

إذا حولنا هذه المقولة إلى نظام العد الثنائي نحصل على:

0101010001110111011011110010000001110000011011110111001101110011
0110100101100010011010010110110001101001011101000110100101100101
0111001100100000011001010111100001101001011100110111010000111010
0010000001100101011010010111010001101000011001010111001000100000
0111011101100101001000000110000101110010011001010010000001100001
0110110001101111011011100110010100100000011010010110111000100000
0111010001101000011001010010000001010101011011100110100101110110
0110010101110010011100110110010100100000011011110111001000100000
0111011101100101001000000110000101110010011001010010000001101110
0110111101110100001011100010000001000010011011110111010001101000
0010000001100001011100100110010100100000011001010111000101110101
0110000101101100011011000111100100100000011101000110010101110010
0111001001101001011001100111100101101001011011100110011100101110

يمكننا الأن أن نحاول فهم الأمن الإلكتروني، وما الذي يعبر عليه الأمن الإلكتروني، وإلى ماذا يشير، فالأمن الإلكتروني، يستعمل حاليا بطريقة واسعة جدا، وذلك بسبب النطاق الواسع الذي اصبح يلعب في دائرة الأمن الإلكتروني، ولهذا ينظر إلى الأمن الإلكتروني في عدة حالات، على أنه تلك

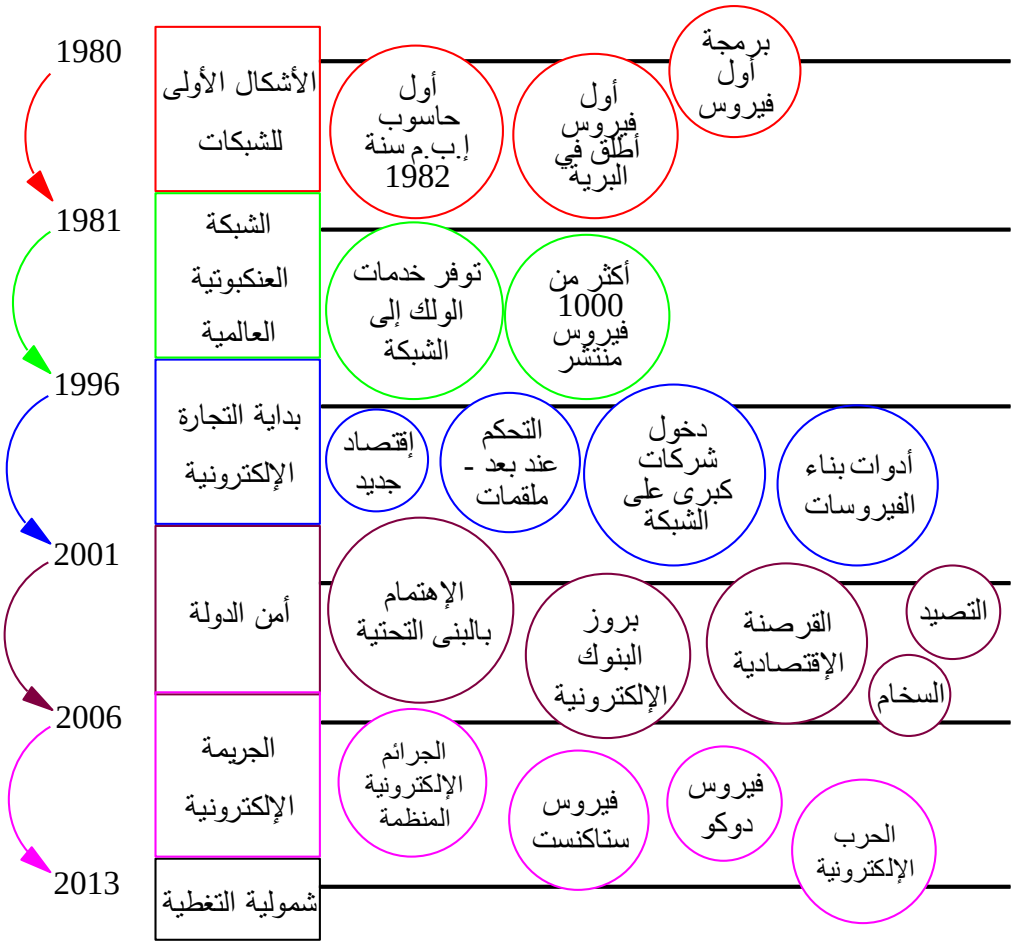
---

[49] Scott Aaronson, "The Limits of Quantum," in ***Information Technology Scientific American***, (Marche, 2008), pp. 62-69.

[50] Eleanor Rieffel, Wolfgang Polak, "An Introduction to Quantum Computing for Non Physicists," in ***Quant-Ph***, (Jeanery, 2000), pp. 1-45.

الإجراءات التي من شأنها الحفاظ على المعلومات، والأنظمة، والهياكل، والسير الحسن لمجموعة من البروتوكولات المبرمجة مسبقا من قبل الإنسان.[51] يجب معرفة أن القضايا التي تتعلق بالفيروسات وطبيعة وجودها، كما عمليات الاستغلال الإلكتروني، لا يعد أمرا جديدا، بل كان موجود من الثمانينيات كما هو موضح في **الجدول رقم 1.3**، ولكن الأمر لم يصبح قضية ذات أبعاد اجتماعية ودولية إلا مؤخرا، ولعل التزايد المستمر في الاعتماد على التقانة يعد أحد ابرز الأسباب لذلك.

لجدول رقم: 1.3



شكل يوضع بعض أهم التطورات في قضايا الأمن الإلكتروني.[52]

(51) Sarwono Sutiko, ***Transforming Security Using COBIT®5*** (The United States of America: Illinois, published by The Information Systems Audit and Control Association, the first edition,2013.), p. 11.
(52) ***Ibid***, p. 13.

ولهذا نجد أن **سارونو سوتوكو** يقسم مراحل تطور الأمن الإلكتروني إلى اربعة مراحل، كل مرحلة لها محددات ومزايا محددة، وقد عرضها وفقا لما يلي:[53]

1. من 1980 إلى 2000، وأطلق على هذه المرحلة إسم : عصر البراءة.
2. من سنة 2000 إلى سنة 2004، وأطلق على هذه المرحلة إسم: عصر الرضى.
3. من سنة 2005 إلى سنة 2010، وأطق على هذه المرحلة إسم: اللحاق بالركب.
4. من سنة 2010 إلى يومنا الحالي، وعبر على هذه المرحلة بسمتجدات الوضع الحالي.

بالإضافة إلى هذا، وفي سياق الأمن الإلكتروني، أو أمن الفضاء الإلكتروني، نجد أن **ناي** قد تكلم على الأمر حين أكد على أن الفضاء الإلكتروني هو فضاء بدون حاكم، وأن الفضاء الإلكتروني بصورته الحالية، يشبه برية الغرب المتوحش(Wild Wild West)، التي لا يوجد بها اي قانون يحكم،[54] ما يمكن أن نراه هنا ينطبق على واقع المجتمع الدولي، والمساهمات النظرية التي ترى أن الفوضى في المجتمع الدولي، سببها عدم وجود سلطة عليا، ففي هذا الفضاء الإلكتروني، عدم وجود سلطة لديها القدرة الفنية الكاملة في السيطرة عليها، تجعل من هذا الفضاء، يحاكي الحياة البرية، أي أن أية شخص يمكنه أن يقوم بما يحلو له، متى توفرت لدي القدرة على ذلك.

كما من جانب آخر، هناك من يرى أن الأمن الإلكتروني، هو ذلك المجال الذي يدرس أي شيء له علاقة بالحواسيب، وذلك العالم المكون من الصفر، والواحد.[55] يمكننا أن نرى الإستعمال الواسع لمصطلح الأمن الإلكتروني، ذلك أن العديد من الأشخاص يستخدم هذا المصطلح للتعبير على العديد من الأشياء التي يمكن أن تتشابه من حيث ميكانيكية عملها، لكن مختلفة من ناحية التقدير القانوني،[56] فالأمن الإلكتروني له علاقة وطيدة ببعض المصطلحات، مثل ما هو الحال مع الجريمة الإلكترونية، والهجمات الإلكترونية، والإرهاب الإلكتروني؛ ففي ظل غياب إجماع فعلي حول مفهوم الأمن الإلكتروني، يبقى

---

(53) ***Ibid***, p. 12.
(54) Joseph Samuel Nye, Cyber Power, ***op. cit***, p. 14.
(55) P.W Singer, Allan Friedman, **Cybersecurity and Cyberwar, What Everyone Needs to Know** (The United States of America: New York, published by Oxford University Press, the first edition 2011.), p. 5.
(56) Tatiana Tropina, Cormac Callanan, **Self and Coregulation in Cybercrime, Cybersecurity and National Security** (The United States of America: New York, published by Springer Cham Heidelberg, in SpringerBriefs in Cybersecurity, the first edition, 2015.), p. 4.

إستخدام هذه المفاهيم بطريقة متداخلة شيء يجب التعامل معه،[57] خاصة على المستوى القانوني، ولما يتعلق الأمر بالحروب الإلكترونية، أو الأسلحة الإلكترونية، إذ أن تحديد المفاهيم هنا سيساعد على لإدراج الأمن الإلكتروني في تخصصات قوى أمنية محددة، ويجنب التداخل في المفاهيم، والوضائف، والصلاحيات.[58]

الجدول رقم: 1.4

	الدوافع	الأهداف	الإستراتيجية المعتمدة
الإرهاب الإلكتروني	التغيير السياسي أو الاجتماعي	ضحايا أبرياء	العنف القائم على استخدام الحواسيب
هاكتفيزم	التغيير السياسي أو الاجتماعي	متخذو القرار وضحايا أبرياء	هجوم حجب الخدمة
القبعات السوداء	تحقيق الذات	أشخاص، شركات، حكومات	برمجيات خبيثة، فيروسات، سكيربتات، دود حاسوبي
الجرائم الإلكترونية	أرباح مالية أو اقتصادية	أشخاص، حكومات	برمجيات خبيثة، سرقة الهوية، حجب الخدمة، الابتزاز، إلى غير ذلك
التجسس الإلكتروني	فوائد اقتصادية أو سياسية	أشخاص، حكومات، شركات	طرق واسعة ومتقدمة من أجل حصد المعلومات
المعلومات الحربية	فوائد سياسية أو عسكرية	الهياكل، الأنظمة الإلكترونية، الخاصة والعامة	طرق واسعة ومتقدمة من أجل الهجوم، أو التأثير على العمليات

جدول يوضح بعض أشكال الأخطار الإلكترونية، والأهداف التي تسعى إليها. [59]

[57] Kristin Finklea, Catharine A. Theohary, Cybercrime: **Conceptual Issues for Congress and U.S. Law Enforcement, in CRS REPORT Prepared for members and Committees of Congress** (January, 2015), pp. 2-17.
[58] Derek E. Bambauer, "**Conundrum,**" in ***Minnesota Law Review***, No 227, Volume 96, (2011), pp, 535-630.
[59] Irving Lachow, "Cyber Terrorism: Menace or Myth?," in ***A National Defense University and Forces Transformation and Resources Magazine***, (April, 2008), pp. 61-81.

كما أضاف **باري بوزن** أيضا، في علاجه لموضوع تطور الدراسات الأمنية في العلاقات الدولية، على أنه هناك مخاطر حيوية جديدة (Bio-Security)، ولهذا برزت هناك العديد من الدراسات التي تتعلق بقضية استعمال الإرهاب المتزايد للتكنولوجيا، وعلى أن الأنترنت أصبحت حقلا جديدا للصراع، ففي سنة 1990، أعلنت رسميا إدارة **كلينتون** على أن الأمن الإلكتروني أصبح يشكل هاجسا حقيقيا للدولة، هذه التحولات، غيرت فعليا، وبطريقة جذرية نظرة الدول إلى الفواعل الغير رسمية في العلاقات الدولية، وطريقة بنائها. [60]

يجب أن نعرف أيضا أن المخاطر، أو التهديدات التي تواجه الأمن الإلكتروني للدول، لا تأتي فقط من قبل المتغير البشري، وسيكون من الغريب فعلا لو قلنا مثلا، أن الطبيعة أيضا أصبحت تشكل تهديدا فعليا للأمن الإلكتروني، والاستقرار التقني العالمي؛ ولعل ابرز هذه الأخطار، والتي سببت أضرار مادية فعلية في أرض الواقع، يأتي من الفضاء الخارجي، ونحن نتكلم هنا بالتحديد على العواصف الجيومغناطيسية (Geomagnetic Storm) التي سبب أضرار كبيرة، للعديد من الأنظمة الإلكترونية، وقنوات النقل الوجي المتعلق بالراديو، كما خطوط نقل الكهرباء، والرادارات، ونحن نتكلم هنا خاصة على المناطق الشمالية من الكرة الأرضية، ويمكن تتبع بعض الأحداث المدونة حتى إلى سنة 1854، وقد تم إعلان أول خبر على أضرار الموجات الجيومغناطيسية الكونية سنة 1940،[61] وفي سنة 1989 تسببت موجات دامت فقط لمدة دقيقة وستون ثانية، في تعطيل كامل لمحطة إنتاج الطاقة الكهربائية في مقاطعة كيبك في كندا، مسببتا بذلك أضرار فاقت المليون دولار أمريكي.[62]

بالإضافة إلى ما سبق، فالموجات الكهرومغناطيسية في اصلها لها دور في عمل الأجهزة التي نحتاجها كل يوم، وبفضلها أيضا، يمكننا أن ننير المدن في الليل، وتشغيل الحواسيب، [63] ولكن هذا لا يعني أنه لا يمكن استخدام هذه الموجات لأغراض عسكرية مثل ما هو الحال مع القنابل التي الغرض منها هو توليد موجات الكهرومغناطيسية (IEM - Impulsion Electromagnetic Pulse)، والتي

---

[60] Barry Buzan, Lene Hansen, ***op.cit***, p. 248.

[61] A.D Alberston, J. M. Thorson, S. A. Miske, "**The Effect of Geomagnetic Storms on Electrical Power Systems,**" in ***IEEE Transactions on Power Apparatus and Systems***, Volume PAS-93(1974), pp. 1031-1044.

[62] Rajbir Kaur Sidhu, **Impacts of Geomagnetic storms on Trans-Canadian Grids,** Master's Thesis, not published (McGill University: Department of Electrical Engineering, 2010), pp. 26-27.

[63] Michio kaku, ***Physics of the Impossible: A scientific Exploration into the World of Phasers, Force Field, Teleportation, and time travel*** (The Unites States of America: Ney York, published by The Doubleday Broadway, the first edition, 2008.), p. 24.

هدفها الأساسي موجه لا من أجل تدمير البنى التحتية، أو القوى البشرية، ولكن موجهة ضد أي نظام إلكتروني من أجل إتلافه، وإخراجه عن الخدمة. [64]

من هنا يمكننا أن نتصور البعد الذي اصبح يلعبه الأمن الإلكتروني في الحياة الإنسانية، فشمولية تأثيره جعلت منه ظاهرة يصعب تحديدها والتحكم فيها، وهذا هو الشيء الذي حاول أن يقوم به الباحث في تقنيات الدفاع الإلكتروني: **شوهواي كزو** (Shouhuai Xu)، لما أراد تأسيس جديد لعلم الأمن الإلكتروني، خاصة وأن دراسة هذا الموضوع لم تؤخذ بجدية كبيرة إلا في سنة 2008، **فكزو** يرى أن المقاربة المناسبة من أجل فهم هذه الظاهرة الجديدة، تكمن في اعتماد نموذج ديناميكي للأمن الإلكتروني كما هو موضح في **الشكل رقم 1.3**، هذا النموذج له مقاربة تحاول فهم تفرع التخصصات التي يعتمد عليها الأمن الإلكتروني، رغم أن هذه التخصصات لا تعتبر نهائية، فهي في تطور مستمر، ويمكنها أن تتغير وفقا لنوع النظام، أو البيئة الذي يعمل فيها النظام.[65]

وفي الحقيقة إذا نظرنا إلى هذا العرض يمكننا أن نرى فيه نوعا من الحقيقة، كما نوعا من المحاكات لما يحصل في العلاقات الدولية، فالأمن الإلكتروني، وبما انه اصبح يُرى على أنه أي آلية، أو استراتيجية، افتراضية، أو مادية، يتم اعتمادها، من أجل إيقاف الأذى، أو السهر على السير الحسن، للأي نظام يعمل على قاعدة إلكترونية، وافتراضية؛ نرى أنه اصبح جزء من المنظومة الدولية، ومثله مثل باقي العلوم، خاصة التي تدرس العلاقات الدولية، يتحتم على أي دارس حاليا، أن يضع في الاعتبار الأمن الإلكتروني، كون العديد من المخرجات التي تحصل في العلاقات الدولية حاليا، هي نتيجة مباشرة، للتطور التقني، أو التعامل الإلكتروني، بداية من التعاملات الاقتصادية، والمعلومات السرية، مرورا إلى الطائرات بدون طيار ، والأقمار الصناعية، وأنظمة الدفاع العسكرية، إلى أي وسيلة تعتمد، ولها قاعدة تقنية إلكترونية.

كما يجدر أن نذكر هنا، أن الأمن الإلكتروني، هو بمثابة مضلة، للعديد من الفروع التي تستند إلى قاعدة تقنية إلكترونية، مثل ما هو الحال مع أمن المعلومات، والأمن الافتراضي، وأمن الأنظمة، والأمن

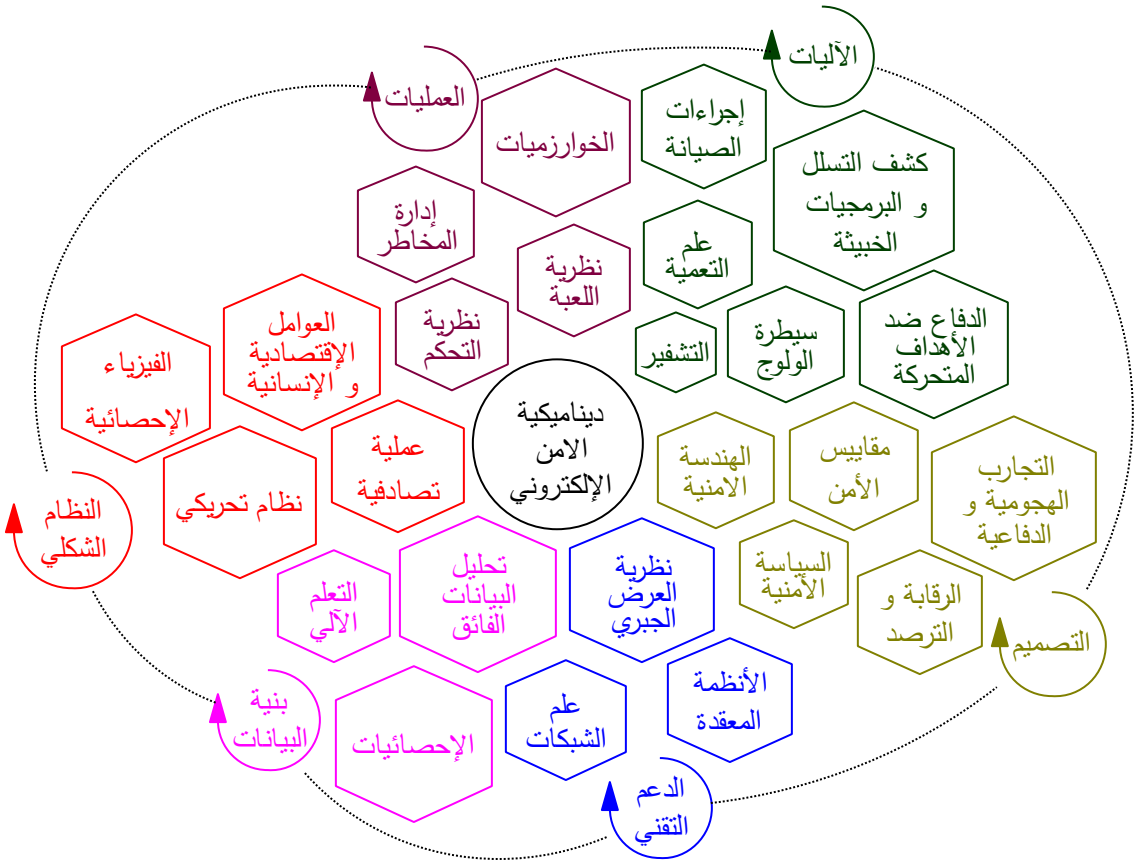
---

(64) Samuel Glasstone, Philip J.Dolan, **The Effects of Nuclear Weapons** (The Unites States of America: published by The United States Department of Defense and The United States Department of Energy ,the third edition, 1977.), pp. 514-532.

(65) Shouhuai Xu, "Cybersecurity Dynamics: A Foundation for the Science of Cyber Security," in: **http://www.cs.utsa.edu/~shxu/socs/**, (Monday, May 02, 2016).

السيبراني، والموضوع هنا، هو دراسة كيفية استخدام كل هذه الوسائل، وفروع الأنظمة التي تستند إلى الإلكترونيات، من أجل الهيمنة العالمية، أو مكافحة هذه الهيمنة.

الشكل رقم: 1.3



شكل يوضح ديناميكية الأمن الإلكتروني.[66]

في الأخير نكون قد فهمنا أنه مهما قام الشخص، أو منظمة معينة، أو أي جهة، بكافة التدابير اللازمة من أجل الحماية، إلا انه في الحقيقة، الخطر لا يزال موجود.[67] وهذا الشيء هو الذي يميز التقانة في العصر الحالي، فبالرغم من كل الإمكانيات التي يمكن تسخيرها، إلا أنه وبكل بساطة يمكن أن تجد أن شخص ما كان يستغل ثغرة الهجوم دون انتظار(Zero-day Attack) منذ فترة، من غير علم احد، ولهذا يمكننا أن نقول أنه إذا كانت العلوم الاجتماعية

[66]Loc. cit

[67] Kevin D. Mitnick, William L. Simon, The **Art of Deception, Controlling the Human Element of Security** (The United States of America: Ney york, published by John Wiley & Sons, the first edition, 2002.), p. 11.

يقال عنها أنها نسبية، وغير دقيقة، فيمكننا أن نقول من جانب آخر أن ميدان الدفاع الإلكتروني، أصبح يعبر على هذه الفكرة بطريقة واضحة جدا، ولا يمكن إنكارها حتى من عمالقة الأمن الإلكتروني في العالم.

1.3.1 الأمن المعلوماتي

الأمن المعلوماتي هو بمثابة امتداد لما كان يحصل في الحياة التقليدية، والتي كانت تتعلق بالقيمة التي يمكن أن تحويها معلومة معينة، هذه المعلومات، يمكن أن تكون ذو قيمة معنوية، أو مادية، أو عسكرية، أو اقتصادية، وما دمنا نتكلم على المعلومات فإننا نتكلم أيضا على طرق التعمية، والتشفير من اجل الحفاظ عليها، ويعد هذا الأمر خطرا، لأنه هناك العديد من الدول التي تفرض أن تشفير المعلومات، لا يتعدى حد معينا من التعقيد، ليكون للدولة، متى احتاجت ذلك القدرة إلى الولوج إلى هذه المعلومات، متى اقتضت الحاجة إلى ذلك، أي أن الدولة تسمح للمستخدم العادي، والشركات، تشفير المعلومات بطريقة تكون للدولة والجهات المختصة فقط، القدرة المادية، والفنية، على فك التشفير؛ مثل هذه الأفكار، تعبر فعلا على التطور، والامتداد الذي حصل في تقدير المعلومات، خاصة أنه ولحد الآن، لم يكون الناس متعودين على هذا النوع من المعلومات، فبعيدا عن التخزين التقليدي للثروة، والمعلومات، أصبح الأمن المعلوماتي، يشكل هاجسا بالنسبة للجميع، تحولت حتى إلى فوبيا عند البعض.

يجب معرفة أن العمل على تشفير المعلومات، أو الخوف على خروج المعلومات، لا يعد امرأ جديدا، ويمكننا حتى أن نصعد إلى حضارة المايا، والتي كانت تستخدم لغة مرمزة في الأنشطة السياسية ونظام الحكم، ولهذا توجب على العلماء فك هذا التشفير (Decipherments) عبر استخدام عدة طرق، تعتمد على البحث في الأثار، ودراسة لسانية للسكان الأصليين.[68] ويمكن حتى أن نضيف هنا أن بعض اللغات الغير منتشرة ساهمت في العديد من المراحل التاريخية أثناء الحروب، مثل ما هو الحال مع استخدام لغات الهنود الحمر من قبل الولايات المتحدة الأمريكية، في الحرب العالمية الأولى، والثانية. وبالطبع لا يمكن المرور على الحربين، بدون ذكر قضية فك لغز آلة إنيغما (Enigma machine)، والذي اعتبرها العديد من المؤرخين المتخصصين في الحرب العالمية الثانية، أحد اهم عناصر خسارة

(68) Prudence M. Rice, ***Maya Political Science, Time Astronomy and the Cosmos*** (The United States of America: published by the University of Texas Press, the first edition, 2004), p.17.

ألمانيا النازية، فالتشفير، والتعمية، وأمن المعلومات، هي حقيقة تاريخية، وما نراه حاليا إلا عبارة عن امتداد لهذه الحقيقة.

عند التكلم على أمن المعلومات، والجرائم الإلكترونية، فإنه يتبادر إلى الأذهان أن الأمر يتعلق، بمجموعة من المعلومات التي كان يجب أن تبقا سرا، ولكن كما وضحنا سابقا، أمن المعلومات، هو جزء فقط من الأمن الإلكتروني. أما فيما يخص المتخصصون في القضايا الأمنية المعلوماتية، والإلكترونية، والحاسوبية، فهم يقدمون ثلاثة مكونات للأمن الإلكتروني:[69]

1. **سرية المعلومات**(Data Confidentiality) :

ويشمل هذا الجانب كل التدابير اللازمة لمنع الاطلاع الغير مصرح به على المعلومات الحساسة، أو السرية.

2. **سلامة المعلومات** (Data integrity):

ويتعلق الأمر باتخاذ كل التدابير اللازمة من اجل منع تغيير البيانات والمعلومات.

3. **ضمان الوصول إلى المعلومات والموارد الحاسوبية** (Availability):

ويتعلق الأمر بالقدرة على الوصول إلى المعلومات مهما كانت متى أراد الشخص المخول له ذلك.

إن الأهمية الكبيرة لأمن المعلومات في الوقت الحالي، جعلت الخوض فيه ضرورة حتمية، إذ أصبح من النادر في الوقت الحالي، أن نجد أي شركة أو منظمة عالمية لا يوجد فيها منصب، مسؤول عن الفرق الخاصة بالأمن المعلوماتي.[70] بل هناك من الدول من يذهب إلى ابعد من ذلك، وذلك عبر العمل على تخزين المعلومات الخاصة بمواطنيهم داخل بلدانهم عوض أن تخزن خارج البلاد، وابرز فعلا يوضح ذلك، هي الإجراءات التي تم اتخاذها من قبل دول البريكس (BRICS)، وتتمثل هذه الإجراءات في إقامة خط أنترنت خاص بها يفوق طوله 34،000 كلم؛ وذلك بسبب قضايا تتعلق بالتجسس، والتجسس الصناعي، والأمني، وحفظ البيانات،[71] وقد اعتبر البعض أن ذلك يعد بمثابة إعلان حرب على الولايات المتحدة الأمريكية في هذا المجال، ويجدر ذكر أن هذا المشروع سيمتد من اقصى شرق

---

[69] خالد بن سليمان الغثير، محمد بن عبد الله القحطاني، **أمن المعلومات** (السعودية، جامعة الملك سعود، نشر من قبل مركز التميز للأمن المعلوماتي، الطبعة الأولى، 2005.)، ص ص. 22-23.

[70] Alexander Kott, Cliff Wang, Robert Erbacher, **Cyber Defense and Situational Awareness, Series: Advances in Information Security** (Switzerland: Published by Springer International Publishing, Volume 62, 2014.), p. 52.

[71] Valentin Mândrăşescu, "BRICS countries are building a "new Internet" hidden from NSA," in: **http://goo.gl/HqYY0w**, (Monday, May 02, 2016).

روسيا، إلى ميامي في الولايات المتحدة الأمريكية، أي أنه سيغطي كافة الكرة الأرضية، ومثل هذه المشاريع ستسمح على سبيل المثال، بإجبار المواقع المشهورة عاليا بتخزين بياناتها داخل الدول التي تحوي المستخدمين، وليس داخل الدولة الأم للشركة.[72]

أما فيما يخص التعاريف التي قدمت من أجل تحليل الأمن الإلكتروني، والتعبير عليه، يمكننا أن نرى أنها جد مختلفة، وتختلف باختلاف النظرة إلى ماهية الأمن؛ فهناك من يرى على أن الأمن هو ذلك المجال المتعدد التخصصات، والذي يدرس الأعمال المتخصصة التي لها علاقة بتطوير وإدماج الآليات الأمنية بمختلف أنواعها، وذلك من أجل الحفاظ على المعلومة المخزنة، من أي تهديد، أو خطر،[73] ويمكننا أن نرى في الشكل **الجدول رقم 1.5**، بعض أهم التعريفات التي قدمت للأمن المعلوماتي.

الجدول رقم: 1.5

المصدر	الأمن الإلكتروني
بيبكين(Pipkin) 2000	عملية الدفاع عن الملكية الفكرية لمنظمة معينة
بلاكلي وآل(Blakley & al) 2002	مجال لإدارة المخاطر، الذي يدرس تكلفة الخطر للمعلومة
أندرسون(.Anderson J) 2003	حس متقدم من الضمان الذي يوازن بين التحكم والخطر
شوماكر وآل(Shomaker & al) 2004	بغض النظر أنه علم قائم، يدرس الأمن الإلكتروني أيضا كل ما له علاقة بعلم الحاسوب، وهندسة الحواسيب، والرياضيات، ونظرية الاتصال، والعلوم العسكرية، والتجارة، والتشفير، والقانون، والأخلاق، والإحصاء، وهندسة البرامج، وطب شرعي الحاسوب، وكل ما له علاقة بالأنترنت.
شارمود وآل(Sherwood & al) 2005	يدرس تمكين الأعمال التجارية الإلكترونية، وكل ما له علاقة بالضمان.
دلاميني وآل(Dlamini & al) 2009	تطور من معالجة بسيطة لبعض المخاطر، إلى إدارة واسعة للتهديدات الكبرة للمنظمة، والتطور الاقتصادي...
شاهينو ومارشانت(Chanhino & al) 2010	هو المجال الذي يتحكم تحديد المجال الآمن للمعلومات، وضمان الامتثال القانوني والنظامي.
كازامي وآل(Kazemi & al) 2012	لا يعد فقط مشكلة تقنية، بل مشكلة فعلية في الإدارة، هدفه الأساسي هو خلق بيئة آمنة للمعلومات.

[72] Karel Vereychken, "Les BRICS déclarent la guerre des câbles contre Londres et Wall Street," in : **http://goo.gl/HKGO13**,(lundi 2 mai 2016).
[73] Sweety Sen, Sonali Samanta, "Information Security," in ***The International Journal of Innovation research in Technology***, No 11, Volume 1 (2014), pp. 224-231.

وايتمان وماتورد(Whitman & Mattord) 2012	حماية الخصوصية، وتوفر المعلومات المخزنة، أو القيد العلاج، أو المتنقلة، وذلك عبر سياسات، وتدريب، وتعليم، والحذر، والتكنولوجيا.

جدول يوضح بعض التعريفات المقدمة للأمن المعلوماتي. [74]

ولكن يجب أن نقول هنا، أنه مثل ما هو الحال مع الأمن الإلكتروني، تحقيق الأمن المعلوماتي الكامل، هو بمثابة وهم يسعى إليه الجميع، ولهذا يقول **بروس شنايدر** (Bruce Schneider) في وصفه لحالة الولايات المتحدة الأمريكية مع قضايا الأمن الإلكتروني وأمن المعلومات أنه:[75]

> "**مع مرور الوقت، سيرى الناس أنه لا جدوى من كتابة قوانين ضد تكنولوجيا معينة، فالاحتيال يبقى احتيال، سواء كان ذلك عبر تشفير الملفات التي تم الحصول عليها بالوسائل التقليدية أو الوسائل الحديثة، فنحن الآن نعيش في عالم تتقدم فيه التكنولوجيا بشكل أسرع من الاجتماعات التي يتم عقدها في الكونغرس، ولهذا يجب أن تكون هناك آليات اسرع في الاستجابة لمثل هذه المستجدات، والتطورات.**"

فالحواسيب تقوم بتخزين المعلومات عنا بطريقة مستمرة، والقليل فقط من الناس يعرف علا مدى ضخامة المعلومات التي يمكن الحصول عليها من الحاسوب الشخصي،[76] وفي سنة 2012 نشرت جريدة نيويورك تايمز مقال يتكلم على كيف تقوم الشركات بجمع معلومات عن المستخدمين، لدرجة أن الشركات أصبحت تعرف وفق انساق شراء معينة، بأن المرأة حامل أو لا، ثم تستعمل الشركة هذه المعلومة كي ترسل عروض، وقسائم تخفيضات للمرأة، من اجل دفعها لشراء منتوجات معينة.[77] لهذا، وفي العديد من الأحيان، ورغم أن إمكانية فشل

---

[74] Yulia Cherdantseva, Jeremy Hilton, "Information Security and Information Assurance: Discussion about the Meaning, Scope, and Goals," in ***Standars and Standarisation – Information Resources Management Association***, Volume 3(2015), pp. 1204-1236.

[75] Bruce Schneider, Secr***et and Lies, Digital Security in a Networked World*** (The United States of America: New York , Published by Wiley Publishing , the first edition, 2000), p. 17.

[76] Bruce Schneider, ***Data And Goliath, The Hidden battle to Collect Your Data and Control Your World*** (The united States of America: Ney York, published by W. W. Norton & Company, the first edition, 2015), p. 15.

[77] **Ibid**, p. 29.

الأنظمة امر مسلم به، إلا أن الأسباب التي تتعلق بالعامل البشري لا يمكن استبعادها أيضا،[78] ولهذا يقول **شنايدر** أنه يمكن النظر إلى هذا النوع من الأمن، والذي يتعلق بأمن الاتصالات، وأمن المعلومات، كسلسلة، وأن قوة كل النظام تقاس بقوة الحلقة الضعيفة من السلسلة، لهذا يجب تامين، وتشفير كل شيء.[79]

لقد أصبح التشفير، أحد أهم ما يميز مجال الأمن الإلكتروني، فإن تعمية المعلومات يساهم بشكل كبير في حماية المعلومات، إذ أن أي شخص يحصل على البيانات المشفرة، عليه بإيجاد الخوارزمية اللازمة من أجل فتح الملف، وأدوات التشفير الموجود حاليا وبعضها مجاني، يسمح لأي شخص بتشفير بياناته بطريقة، لن تستطيع حتى اقوى الحواسيب كسرها، وكيف لا ومكتب التحقيقات الفدرالي(Federal Bureau of Investigation - FBI) في الولايات المتحدة الأمريكية يصرح بشكل رسمي وينصح بدفع *الفدية الإلكترونية(Ransomware) إلى كل شخص تم تشفير ملفاته بطريقة غير قانونية، بل حتى المكتب نفسه قام بدفع الفدية، بعد تشفير بعض الملفات الحيوية التي كانت تحوي بعض المعلومات عن المساجين ، والقضايا.[80]

يمكننا أن نعرف من هنا حجم ما أصبح يمثله التشفير للأمن المعلوماتي، والإلكتروني، بل أصبح التشفير يمثل ثقافة الأقوى، وقد تجسد ذلك في ظاهرة السكيدا 3301، والتي تعد كأكبر لغز مفتوح على الواقع، وهو موجه خاصة، لمتخصصي التشفير(Cryptography)، والتعمية (Cipher)، *والستيغانوغرافي (Steganography)، مثل هذه الأحداث، والمناسبات، توضح لنا أن العالم قد تغير.

---

(78) Solange Ghernaouti, ***Cyber Power, Crime and Conflict and Security in Cyberspace*** (Switzerland: Published by EPFL Press, the first edition, 2013), p.351.

(79) Bruce Schneider, ***Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code*** (The Unites States of America: Ney York, published by Wiley Computer Publishing, John Wiley & Sons, Inc, 1996.), p. 181.

(80) Paul, "FBI's Advice on Ransomware? Just Pay the Ransom," in: ***https://goo.gl/3Qtjm8***, (Monday, May 02, 2016).

- الفدية الإلكترونية(Ransomware): يقوم المخترق بتشفير الملفات في حاسوب الضحية، فتصبح غير قابلة للاستعمال، ويطلب المخترق فدية إلكترونية مقابل إعادة فك التشفير على الملفات لتصبح متاحة من جديد.
- الستيغانوغرافي (Steganography): فن إخفاء المعلومات في الصور.

الصورة رقم: 1.0

أول شكل مشفر يمثل سكيدا 3301 (Cicada 3301)،

من طرف منظمة سرية سنة 2012(cicada3301.org)

وتوضح لنا أيضا أن معايير القوة قد تغيرت كليا، ففي هذه الساحة، وبالرغم أنه يمكن أن نقول أن للدولة إمكانيات كبرى من ناحية القوة الحاسوبية، إلا انه وبمجرد نقرات بسيطة، يمكن لأي شخص أن يشفر معلوماته، ويجعلها غير قابلة للولوج، حتى لو استخدمت حواسيب كمية لمحاولة كسرها.

وفي نفس السياق التشفير، وحماية المعلومات، فقد برزت العديد من الطرق التي تساعد على الحفاظ على المعلومات على كافة المستويات، إذ برزت طرق لحماية المعلومات حتى عند الإجبار، واستخدام القوة، فقد برز في هذا الصدد ما يسمى بالتشفير القابل للنكر (Deniable Encryption)، وهي عملية تشفير مزدوج لنظام معين، التشفير الأول هو التشفير الفعلي، ويؤدي إدخاله إلى الولوج إلى الملفات الحقيقية، أما التشفير الثاني فهو موجه للإنكار، وعند إدخاله فإنه يوجه الشخص إلى مكان آخر ليتم تضليله؛ منا هنا، يمكننا أن نقول أن أمن المعلومات، مثله مثل الأمن الإلكتروني، يعد أحد أهم ما يميز القرن الحالي، كما يعد أيضا امتدادا طبيعيا للوسائل التقليدية للإكراه، والصراع الدولي، والمجتمعي، يعد جزءا من الكل، ويشكل أحد الهواجس المعاصرة.

1.3.2 الأمن الموزع

كأي موضوع يتكلم على مخاطر التطور التكنولوجي، وعن الدور الذي أصبحت تلعبه التكنولوجيا في الحيات الدولية، لا يمكن المرور على ما يسمى الأمن الموزع. يعد الأمن الموزع لحد الآن أحد أخطر التطورات التي حدثت في الساحة الأمنية على المستوى الدولي، وذلك عبر توفر الأدوات في تصنيع أو برمجة أسلحة معدة خصيصا للاستعمال الخاص، فحاليا أصبحت هناك العديد من الأدوات المتوفرة للعامة مثل برامج خاصة تسمح للأشخاص بصنع ملقمات خاصة ومشفرة من اجل قرصنة الأشخاص مثل البرنامج الشهير نجرات (Njrat - Remote administration tool). والذي يمكن أن نقول أنه متوفر للجميع ولا يحتاج أي خبرة في البرمجة من أجل استخدامها لدرجة أنه يمكن حتى لشخص لم يستعمل الحاسوب من قبل أن يعرف كيف يستخدمه في بضعة دقائق،

هذا النوع من البرامج يسمح للشخص الذي أرسل الملقم أن يحصل على صور، ورقنات لوحة المفاتيح، والملفات، والعديد من المعلومات من الضحية أو الشخص المستهدف، [81] كما أن الوسائل الحديثة لتشفير الملفات، جعلت من الصعب الكشف عن الملفات المفخخة، أو الملفات التي يتم دمجها داخل برامج لديها تصريحات معترف بها، ويتم تثبيتها مع تثبيت البرنامج أو فتح الملف. ولقد أثبتت التقارير الأخيرة، الانتشار الواسع لهذا النوع، أي البرامج المتطفلة التي لديها ميزة الغدارة عن بعد، كما صرحت فاير أي (FireEye)، وهي شركت متخصصة في الكشف المتقدم للمخاطر الإلكترونية، حين صرحت أن: [82]

> **"هذه الهجمات في تزايد مستمر خاصة في المنطقة الأوروبية ومنطقة الشرق الأوسط، وأوضحت التحاليل الأخيرة على أن الجزائر والكويت تترأس قائمة الأشخاص أو الملقمات أو الخوادم المتحكمة في الحواسيب في العالم".**

---

[81] Kjetil Tangen Gardåsen, **Detecting Remote Administration Trojans through Dynamic Analysis using Finite-State Machines**, Master's Thesis, not published, Norway, (Gjøvik University College: Department of Computer Science and Media Technology, 2014.), pp. 38-43.

[82] Regional Advanced Threat Report ,Europe, Middle East and Africa 1H2014, FireEye, (https://www.FireEye.com), 2014, p. 17.

يمكننا أن نرى أنه رغم أن الجزائر مصنفة في المرتبة رقم 103 من حيث سرعة الاتصال في العالم، والمرتبة رقم 134 من حيث سرعة الاتصال على شبكات الهواتف، والمرتبة رقم 50 بحوالي 23 بالمئة فيما يخص المنازل التي تتوفر عليها شبكة الأنترنت، والمرتبة رقم 133 من حيث عدد الأشخاص الذين يستعملون الأنترنت.[83] إلى جانب هذا فالجامعات الجزائرية مثل ما هو الحال مع جامعة بومدين للعلوم والتكنولوجية وجامعات أخرى متخصصة لديها تصنيف عالمي يتراوح بين 1700 و23000 .[84] ولكن رغم هذا نرى أن الجزائر تصنف في العديد من المرات تصنف كأحد الدول الأوائل من حيث الهجمات الإلكترونية، لذا يبدو لنا هنا أنه من الواضع أن المعضلة الإلكترونية تعبر عن نفسها بطريقة مباشرة، ذلك أن ميزة هذا النوع من التقانة تجعل استخدام أدوات معينة أن تعلمها امر متاح للجميع، الأمر الذي يصعب قياسه إذا ما تكلمنا بالمقارنة مع دول أخرى أكثر تطورا، مما يوحي إلى دوافع معينة متوفرة، لكن وكما سنوضح لاحقا مع هجمات حجب الخدمة، هناك العديد من المؤثرات التي لها دور مباشر في طريقة عمل القراصنة والمقاربات التي يتم اعتمادها.

أما الأمر الثاني فيتمثل في شيء أكثر خطورة، وله علاقة بالطابعة الثلاثية الأبعاد؛ فالطابعة الثلاثية الأبعاد هي أداة يتم استعمالها، من أجل طباعة قطع، وأشكال معينة عبر استخدام مواد مختلفة قابلة للاستخدام وفقا لنوع الطابعة، ويعد هذا الأمر قفزة في كبيرة في التطور التكنولوجي، ويقول المهندس في برمجيات الجرافيك **كيريل فيديمش** في هذا الصدد:[85]

> "**أشعر بالحماسة تجاه العمل على الأشياء المادية، كنوع من التغيير، لم أكن أبدا صانعا للأشياء لكنني دائما أردت أن أكون كذلك ... أعتقد أنه من الممتع أن تصل إلى التقاطع الذي تستطيع فيه أن تجمع بين المعرفة بعلوم الحاسوب والإلكترونيات، وبين المواد الملموسة.**"

لكن الأمر الذي بدأ في طباعة أسلحة خفيفة به في المنزل وبدون أن تكون لديه أي خبرة في مجال تصنيع الأسلحة، ويمكنه فقط القيام بذلك عبر استخدام الطابعة الثلاثية الأبعاد المتوفرة في السوق بأسعار مناسبة ومتاحة للجميع، خاصة إذا ما راينا ما يمكن أن تقوم به الطابعة، وتتم العملية عبر استخدام ما

---

[83] Broadband for all a Report, Switzerland, Geneva, ***Broadband Commission for Digital Development***, 2015. pp. 90-104.

[84] Ranking Web of University, in: ***http://www.webometrics.info/en/Africa/Algeria***, (Wednesday, April 27, 2016).

[85] نيل سافاج، "بناء الفرص"، **الطبيعة**، العدد 22 (يوليو،2014)، ص ص. 93–94.

يسمى بالبصمة الزرقاء (Blueprint)، أي ملف يتم اعتماده من أجل طباعة النموذج الثلاثي الأبعاد، والشكل التالي يمثل أحد النماذج الذي قامت بإعداده منظمة الأمن الموزع للمصادر المفتوحة: [86]

الصورة رقم: 1.1

أول نموذج فاعل أطلق عليه اسم المُحرر (The Liberator)
تم طباعته كليا، عبر استخدام طابعة ثلاثية الأبعاد متوفرة للعامة. [87]

هذا الأمر الجديد خلق شيء لم يكن موجود من قبل، وهو الأسلحة المفتوحة المصدر (Open Source Weaponry)، ففي الأصل التصاريح المفتوحة المصدر هي تلك التصاريح التي لها علاقة بالملكية الفكرية، وحقوق النشر، والاستعمال، وإعادة الاستعمال، والاستغلال التجاري، أو الغير تجاري، لكل المعدات، أو برمجيات، أو أي قيمة مادية، أو معنوية، والتي يمكن استعمالها من اجل تحقيق فوائد معينة، والتي حقوقها محفوظة في دولة معينة أو في منظمة دولية معينة، أو على الشبكة الافتراضية، مثل هذه التصاريح تشكل العمود الفقري للتعاملات واستغلال الموارد التجارية التي يملكها أشخاص أو منظمات أو دول. ولكن لما يكون التصريح مفتوح المصدر، فإن هذا يدل على أن الشيء المراد استغلاله، أو المنتج، أو أن القيمة المعنوية، أو المادية، يمكن استخدامها بشكل حر، ويمكن استعمالها أو التعديل عليها لأغراض شخصية أو اقتصادية، بدون الرجوع إلى الصانع أو المنِتج الأصلي. فمن بين الأشياء التي تجعل من المصادر المفتوحة امر جيدا، هي أنها تساعد على دفع الإبداع إلى الأمام،

(86) 3D Model of the Liberator, in: ***http://defdist.tumblr.com/page/2***, (Wednesday, April 27, 2016).

(87) The Liberator, in: ***https://defdist.org/***, (Wednesday, April 27, 2016).

خاصة لما يتعلق الأمر بالأنظمة الإلكترونية وأنظمة التشغيل، إذ أن المجتمع الإلكتروني يساهم بشكل مستمر في تحسين هذه الأنظمة وجعلها أكثر ملائمة وتطورا. [88]

الصورة رقم: 1.2

شعار منظمة الأمن الموزع (Defense Distributed). [89]

ولهذا سعت المنظمة، والتي مقرها في الولايات المتحدة الأمريكية، إلى خلق العديد من النماذج المفتوحة المصدر لأسلحة عديدة يمكن طباعتها، عبر استخدام طابعة ثلاثية الأبعاد، وفي المقدمة حصنت المنظمة نفسها عبر تأكيدها على التعديلات التي تم إقرارها سنة 1791 تحت عنوان وثيقة الحقوق، خاصة التعديل الثاني والذي ينص على: [90]

> "**أن وجود ميليشيات منظمة بشكل جيد داخل الدولة يعد أمرا ضروريا لأمن الدولة، ولهذا لا يحق لأي أحد أن يتعرض لحق الشعب في امتلاك أسلحة**".

وقد قُدم هذا التعديل لضمان أمن الشعب من الدولة، كون الاستبداد دائما يبدأ عند احتكار القوة، ولهذا أرادت منظمة الأمن الموزع، أن تعتمد على هذا المنطلق من أجل توزيع النماذج الخاص بها، لكن يجدر الذكر هنا أنه ليس كل الدول لديها نفس القوانين فيما يخص تصنيع الأسلحة، لأغراض خاصة، أو لأغراض تجارية. كما أنه تم الضغط على مؤسس المنظمة **كودي ويلسون** (Cody Wilson) من طرف مكتب القضايا العسكري والسياسية في الولايات المتحدة الأمريكية، وقدمت حجة رسمية تنص وتؤكد على أن نقل النماذج الأسلحة وتوزيعها لا يتوافق والقوانين التي تحكم التبادل الدولي للأسلحة (- ITAR

---

[88] Chris, Dibona. Sam, Ockman. Mark, Stone, **Open source, Voice From the Open Source revolution** (The United States of America: California, O'Reilly & Associates Inc, the first edition ,1999), p. 10.

[89] Official Logo of Distributed Defense, in: ***https://defdist.org/***, (Wednesday, April 27, 2016).

[90] United States Constitution. ***Bill of right rectification***, Second Amendment, 1791.

International Traffic in Arms Regulations)، والقوانين التي تتعلق بتصنيف الأسلحة من المستوى الثاني مثل البنادق الرشاشة الهجومية.[91] وأجبر على سحب نموذج المُحرر من التحميل بعد أن تم تحميله لأكثر من 100.000 مرة، لكن بلا فائدة كون العديد من الموقع تكفلت بإعادة تحميل الملف وإعادة نشره من جديد(The Pirate Bay Website)،[92] في إشارة أنه حتى لو كانت هناك العديد من القوانين التي تمنع أو ستمنع مستقبلا التناقل بهذا النوع من البصمات، إلا أنه لا يمكن لأحد السيطرة عليها حاليا.

ووفق هذه المحاولة لتوضيح مفهوم الأمن الموزع، يكمن الهدف هنا في الطفرة والتقدم التكنولوجي أكثر منه في الأحداث الجارية أو التي حصلت، وهذا ما يوافق عليه الصحفي المتخصص في القضايا التكنولوجية **نيك بيلتون** (Nick Bilton)، حيث يقول:[93]

> "**أكان الأمر قانوني أو لا، أنا أؤمن أنه بعد 15 سنة، سيتملك كل شخص طابعة ثلاثية الأبعاد في المنزل من أجل إعداد أشياء خاصة مثل الأواني وما شابهها، فمثل ما حصل في الطفرات التكنولوجية التي عايشناها، لا يمكن إيقاف هذا الأمر حاليا، البعض سيختار طباعة الأواني، والبعض الآخر مثل كودي، سيقوم بطباعة الأسلحة**".

وهذا ما تؤكده بعض الإحصائيات، إذ المختلف الحكومات حول العالم بدأت الاستثمار في مثل هذه التكنولوجية، ففي 2012 منحت شركة أمريكا ميكس (America Makes) في أوهايو، 30 مليون دولار في صورة تمويل حكومي، و40 مليون أخرى في القطاع الصناعي، هذا إلى جانب العديد من المشاريع الأخرى الممولة من قبل وكالة المشروعات البحثية، ووكالة ناسا التي بدأت تبحث عن إمكانية إرسال هذه التكنولوجيا للفضاء (القمر، المريخ) لبناء البيوت عبر استخدام موارد متاحة. يضاف إلى هذا؛ إعلان

---

(91) United Stated Department of State, Bureau of Political-Military Affairs, office of Defense Trade controls compliance, Washington, D.C, A replay to Mr Cody Wilson about Distributed Defense, 2013.

(92) Andy Greenberg, "3D Printed Gun's Blueprints Downloaded 100,000 Time In Two Days," in: ***http://goo.gl/RqGcOr***, (Saturday, April 30, 2016).

(93) Erin Lee Carr, 3D Printed Guns, Documentary, in: ***https://youtu.be/DconsfGsXyA***, Saturday, Motherboard, Vic Media Inc, (Tuesday, July 12, 2016).

سنغافورة عن استثمار 400 مليون دولار على مدى خمسة سنوات، على أبحاث حول الطابعة الثلاثية الأبعاد، وأعلنت الصين أيضا عن تخصيص 250 مليون دولار لمثل هذه الأبحاث على مدار ثلاثة سنوات القادمة، كما أعلن مجلس استراتيجية التقنية، ومجالس الأبحاث في المملكة المتحدة عن تخصيص ما يقارب خمسة عشر مليون دولار لهذا النوع من الأبحاث. [94]

لقد أصبح الأمن حاليا وخاصة في خضم مفهوم الأمن الموزع يعد أمرا مفتوح، ولا يمكن التكهن به، ذلك أن الوسائل التي يتم اعتمادها من إلحاق الضرر كما رأينا، أصبحت مفتوحة أكثر فأكثر على العامة، كما أن طبيعة النظام العالمي نفسه الذي اصبح يعتمد بشكل كبير على التقانة له دورا كبيرا في ذلك، فلامركزية القوة التي يمكن أن نفهمها عبر الإفرازات المحتملة لهذا النوع من التكنولوجيا، سيشكل تهديدا فعليا لهيمنة الدولية، كما سيشكل تهديدا لأطماع أي دولة أخرى، ففي ظل الصراع من اجل الهيمنة القائم بين الدول، تبقى مثل هذه الأنواع من التقانة، كسلاح بين بين العديد من الأسلحة التي وفرها التطور التكنولوجي في الحصر الحالي.

1.4 الهيمنة الإلكترونية

لقد لعبت الثورة التقنية دورا مهما، إذا لو نقل جوهريا، في تغيير الذهنيات السائدة، فقبل بروز الترانزستور، وما تبعه من تقدم تقني، وتراكم في الاختراعات، والتطبيقات الإلكترونية، كانت الهيمنة في العلاقات الدولية تستند إلى الوسائل التقليدية للإكراه مثل ما هو الحال مع القوة العسكرية، والاستراتيجية الخطية للهجوم العسكري، ويمكننا حتى إضافة المتغيرات الاقتصادية الحالية، ويمكننا أيضا إدراج الهيمنة العالمية التي تستند إلى الأسلحة الشبه تقليدية، والحديثة على غرار القنابل الذرية، والهيدروجينية، والنووية؛ هذه الوسائل يمكن أن نقول أنها تشترك في شيء واحد ، وهي احتكار الدولة، أو الحكومة لهذا النوع من القوة والتقنية، وبذلك فإن أي عملية تهدف إلى الهيمنة في العلاقات الدولية، ستكون نتيجة مخرجات، وقرارات تقوم بها الدولة؛ ولكن حاليا يمكننا أن نرى أن قواعد اللعبة قد تغيرت، فالهيمنة لم تعد فقط تلك التي لها علاقة بالسيطرة على الأرض، والموارد، والأشخاص، فقد أصبح هناك عالم افتراضي موازي، يعبر عن التقدم التقني، والعالم المتغير، ولهذا تبين للجميع أنه هناك مجال جديد في الصراع على

---

[94] نيل سافاج، ***مرجع سابق***، ص ص. 93-94.

الهيمنة العالمية، مجال لم تعد الدولة قادرة على احتكاره، ولكن رغم ذلك تعد الدولة أهم مساهم في هذا السباق نحو الهيمنة كما سنرى لاحقا فيما يخص القوة الحاسوبية.

لا يمكن لأحد أن يتكلم على الهيمنة في العلاقات الدولية حاليا، أو أن يبدي رغبته في الهيمنة الدولية، بدون أن يتكلم على الهيمنة الإلكترونية إذ اصبح يمثل التفوق التكنولوجي أحد أهم هواجس الدول الكبرى، وهي تعمل جاهدا من أجل إيصال فكرة للآخر على أنها الأقوى في هذا المجال، فالتفوق التكنولوجي، يرسل رسالة واضحة للآخر على الهيمنة والقدرة على المنافسة، ونتكلم هنا على التوفق الفائق القدرة، والذي لا يمكن أن يكون متاح للعامة، لأسباب تتعلق بالتكلفة الكبيرة جدا التي يجب توفرها من أجل صنع الهياكل، كما الكادر المتخصص الذي يجب أن يتوفر من أجل إدارة هذه الأنظمة، فالتطور التكنولوجي غير فعلا النظرة إلى القوة، وكيفية تحقيق الهيمنة،[95] إذ أن القوة لطالما كان لها مرجعية مادية، عددية، تكنولوجية، أما حاليا أصبح ينظر إلى القوة أكثر بالطريقة التي تسمح بالحفاظ على المصالح القائمة، أو القدرة على الحفاظ على الاستمرارية في ظل ذلك الهامش الحتمي للخطر، والذي يجب قبوله ، والتعامل معه، فالهيمنة الإلكترونية تعدد أحد أشكال الصراع الدولي الصاعدة، ذلك الصراع الذي سيعتمد على تكنولوجيات متقدمة.[96]

يمكن فهم هذا السباق الشرس نحو الهيمنة الإلكترونية، والسباق نحو القوة الرقمية، في السباق العلني بين القوى العظمة في العالم الإلكتروني، مثل الصين والولايات المتحدة الأمريكية، وتترجم هذه المنافسة في من يملك اقوى التقانة في العالم في ما يسمى حاليا بتصنيف الخمسمئة (Top 500)، هذا التصنيف يعتمد على القوة الحاسوبية المربوطة بنظام واحد، وليس كتلك التي تسمى بالحوسبة الموزعة(Distributed computing)، فالحوسبة الموزعة هي عبارة عن عمل خيري يقوم على تحميل العديد من الأشخاص برنامج معين، ويقومون بتخصيص جزء من القوة الحاسوبية لديهم في المنزل، لأغراض تتعلق بالبحث الطبي، أو العلمي، فكل هذه الحواسب التي تشترك في معالجة مسائل حاسوبية، تشكل الحوسبة الموزعة؛ عكس الحواسيب التي تدخل في التصيف العالمي للقوة الحاسوبية، والتي لا تعتمد إلا على مواردها الخاصة القائم على القلوب، وعلى نظام واحد تعمل عليه.

---

(95) John Law, **A Sociology of Monster, Essays On Power, Technology And Domination** (United Kingdom: London, published by Routledge, the first edition, 1991.), p. 103-110.

(96) Jhon Arquilla, David Ronfeldt, **In Athena's Camp, Preparing For Conflict in Information Age** (The United States of America: Washington D.C, Published by Rand, the first edition, 1997.), p. 44.

يجب أن نعرف هنا، أن النظر إلى التصنيف لا يجب أن يكون من زاوية القدرة الحاسوبية، بقدرة التطبيقات التي يمكن أن يتم اعتمادها، وتطويرها، استنادا إلى هذه القدرة الحاسوبية، فمثلا نجد أن تيانهي-2 (Tianhe-2)، يعد أقوى حاسوب في العالم حاليا من حيث القدرة الحاسوبية (حوالي 3.12 مليون قلب – 33.8 بيتافلوب)،[97] وهو موجود حاليا في الصين، وبالتحديد في مقاطعة غواندونغ (Guangdong) الذي يوجد بها المركز الوطني للحواسيب الفائقة، لكن الذي يهنا هنا هو أن هذا الحاسوب الفائق هو ملك للحكومة الصينية، ويتم تسييره من قبل جامعة التكنولوجيات الدفاعية.[98] هذه القدرة الحاسوبية الكبيرة تعد جد مهمة في عالم البحث العلمي وتطوير تكنولوجيات الدفاع، والمحاكات العسكرية، والأهم من ذلك، تعد جد مهمة في ظل الهيمنة الإلكترونية، أو أي حرب إلكترونية أو معلوماتية محتملة في المستقبل، فالقوة الحاسوبية لا يجب النظر إليها كأرقام فقط، بل يجب النظر إلى التطبيقات التي يمكن أن تعتمد على هذه القدرة، خاصة التجارب الأمنية الإلكترونية مثل ما هو الحال مع هجوم الطاقة العمياء.

يوضح **الشكل رقم 1.4**، وجود سباق فعلي من اجل الهيمنة التقنية في العالم، فمثل ما كان الحال من قبل مع سباق التسلح والذي لا زال مستمر إلى حد الآن، يمثل هذا الشكل دليلا على السباق من أجل امتلاك ما هو اقوى في المجال التكنولوجي، يمكننا رؤية أن الولايات المتحدة في المرتبة الأولى بحوالي 39 % من حيث العدد، والقوة الحاسوبية، ثم تأتي الصين بعدها مباشرة بحوالي 21%، لكن رغم هذا يمكن رؤية أن الصين لديها أكبر علبة من ناحية الحجم في إشارة إلى الحاسوب تيانهي-2. [99]

لقد عُبر على الهيمنة على أنها تلك العلاقات الاجتماعية، والرمزية (Symbolic Domination) التي تتجذر في الحياة الاجتماعية للناس، مسببتا بذلك تغيرات نمطية، وذهنية بطريقة جذرية في حياة الناس، [100] كما هناك من يرى أن الهيمنة تتمثل في السيطرة (Hegemony) التامة لدولة معينة، أو مجموعة من الأشخاص، على جماعات أخرى أو دول أخرى، كما يمكن حتى التعاطي مع الهيمنة بطريقة

---

[97] Brian TSAY, "The Tianhe-2 Supercomputer: Less than Meets the Eye?," in **Newsletters**, (July, 2013), pp. 2-6.

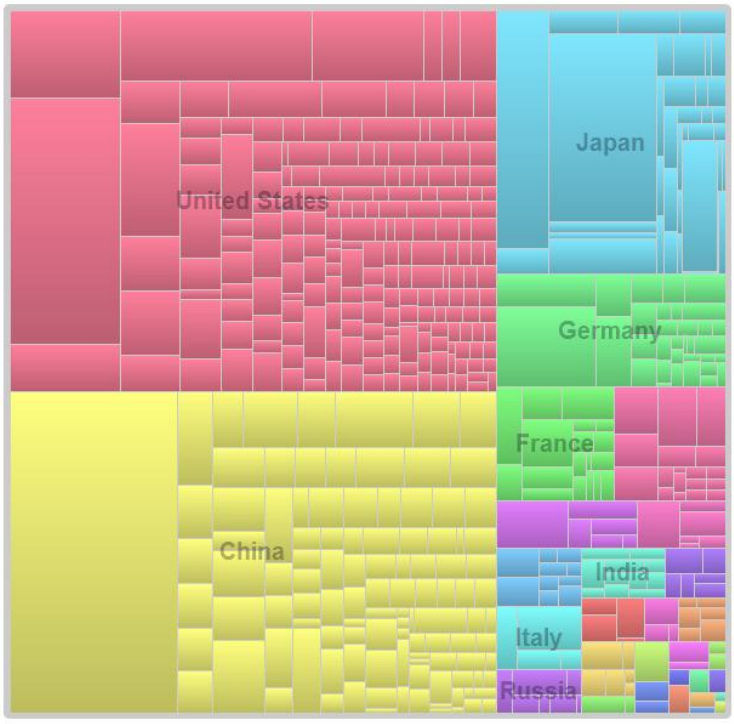
[98] Jack Dongarra, "Visit to the National University for Defense Technology Changsha, China," in O**ak Ridge National Laboratory**, (June 3, 2013), pp. 1-18.

[99] Jack Dongarra, Erich Strohmaier, Horst Simon, "the Top 500 List," in: ***http://www.top500.org***, (Monday, May 09, 2016).

[100] Michael Burawory, "The Roots of Domination: Beyond Bourdieu and Gramsci," in ***Sociology***, No 2, Volume 42(2012), pp. 187-206.

أكثر دقة، ويمكن أن نجد ذلك في تعاطي **أنطوان غرامشي** (Antonio Gramsci 1891-1937) مع مسالة الهيمنة الثقافية، والتي تعبر عن الاعتراف بشرعية النظام القائم والمسيطر بسبب الهيمنة الثقافية، [101] فالهيمنة لها عدة أشكال، وتعالج قضايا متعددة، كما سنرى فيما بعد مع الجيومعلوماتية، لكن الواضح هنا، هي أن الهيمنة قائمة على السيطرة، والملكية مهما كان نوعها.

الشكل رقم: 1.4



خريطة تناسبية (Treemap) تمثل الدول الرائدة في مجال الحواسيب الفائقة القدرة. [102]

يمكننا أن نفهم هنا، وفضل المفاهيم، والمعطيات التي عرضناها، أن الهيمنة الإلكترونية، مثلها مثل المفاهيم الأخرى للهيمنة، فإنها تشمل على الرغبة في السيطرة على الآخر، وينعكس ذلك في مدلول القضايا التي تعالجها الهيمنة الإلكترونية، أو القضايا التي تدخل في حيز الهيمنة الإلكترونية، ففي رؤية معظم الدول، فإن ما تقوم به، يدخل في إطار سيادتها الخاصة، كما أن التعبير على الهيمنة الإلكترونية يصعب إيجاده في الخطاب السياسي، كون هذه الهيمنة هي عملية غير مباشرة تقوم بها الدول، عبر

---

[101] عزمي بشارة، "عن المثقف والثورة،" **تبين**، العدد 4(ربيع،2013) ، ص ص. 128- 142.

[102] خريطة تناسبية (Treemap) تمثل الدول الرائدة في مجال الحواسيب الفائقة القدرة، في: ***http://www.top500.org/statistics***، (الإثنين، 09 أيار، 2016).

القيام بالعديد من العمليات الخفية، وأساليب الضغط؛ مثل ضغط الولايات المتحدة الأمريكية على شركة انتل(Intel) كي لا تبيع كميات كبيرة من المعالجات للصين لأنها ستستعملها لأغراض تتعلق بالأبحاث النووية، أو رفض جهاز الاستخبارات البريطاني (MI6 – section 6،Military Intelligence) استخدام حواسيب تم تصنيعها في الصين لأنها صنعت بطريقة يسهل خرقها، ونفس الأمر يتعلق رفض العديد من الدول القيام بعمليات الاستيطان الاقتصادي(Delocalization of Industry) في الدول الأخرى لتجنب نقل أي تكنولوجيات تعد متقدمة لدولة منافسة. لهذا يمكننا أن نقول أن الهيمنة الإلكترونية، ما هي إلا امتداد للأشكال التقليدية للهيمنة، بطرق جديدة، ووسائل جديدة، وأهداف جديدة أكثر عمقا.

1.4.0 الحرب الإلكترونية

تعد الحرب الإلكترونية بمثابة القلب النابض الذي يحرك الهاجس الأمني في العصر الحالي، إذ هناك من ينظر إلى الحروب الإلكترونية، كعرين الوحش الذي لا يمكن معرفة مكانه، ولا يمكن السيطرة عليه، فالتحولات الكبيرة التي حدثت في التكنولوجيا، جعلت بروز مثل هذا المصطلح أمرا حتميا لا يمكن تجنبه، كما أن بروز هذا الحقل البحثي، نتج عنه أيضا بروز العديد من الحقول التي لها علاقة بالحرب الإلكترونية، خاصة تلك التي تدرس الجانب القانوني للحروب الإلكترونية، وتلك التي تتعاطى مع مواضيع جد معاصرة، مثل ما هو الحال مع الأسلحة الإلكترونية. إن النظر إلى الحرب الإلكترونية، هي بمثابة محاولة لفهم مختلف الطرق التي يتم اعتمادها من اجل إلحاق الضرر، ودراسة مختلف الأسلحة التي يمكن استعمالها في هذا الصدد، إذ يجب معرفة أنه لا يمكن وضع قائمة كاملة لهذه الأسلحة، أو مختلف الطرق التي يمكن اعتمادها في هذه الحرب، كون التقانة في تطور مستمر، ونفس الأمر ينطبق على قواعد البيانات التي تقوم بإحصاء الأسلحة الإلكترونية، وبالإضافة إلى هاذا، يجب أن لا ننسى أيضا أن الحرب الإلكترونية لها علاقة بالهياكل الفيزيائية للأنظمة، في تعبير واضح كما قلنا سابقا، على أنه لا أحد يمكنه السيطرة بشكل تام في هذا المجال. يمكننا أن نقول أولا أن طبيعة الحرب ليست لها علاقة فقط بالتطور التقني، رغم أن التطور التقني له دور كبير في تغيير طبيعة الحروب، وهذا ما أكده **ميتشيو كاكو** حين تكلم على التطور الحضاري إذ قال:[103]

[103] Michio Kaku, ***Parallel Worlds, A Journey Through Creation , Higher Dimension, and the Future of the Cosmos*** (The United States of America: New York, published by DOUBLEDAY, the first edition, 2004), p. 309.

"سيصبح للدولة دورا اقل أهمية، وستسقط الحدود التجارية، ليتجه العالم نحو صيغة يوطد فيها الاعتماد المتبادل بطريقة أكبر، ولا توجد دولة لها القدرة في إيقاف هذه الحتمية ... يبدو أن الحروب ستكون دائما معنا، لكن طبيعة الحرب في حد ذاتها ستختلف بسبب بروز وصعود أكبر للطبقة الوسطى في العالم، والتي ستكون لديها قوة أكبر"

يمكننا أن نفهم هنا، الطبيعة المتغيرة للحروب، ولعل الزيادة الكبيرة في الاعتماد المتبادل، ستجعل من الصعب جدا التعامل مع الصراعات المستقبلية، بالطريقة التقليدية، إذ نجد حتى **صن تزو** يؤكد على أهمية احتلال المدن بدون إلحاق الضرر المادي لها، كما الأهمية الاقتصادية لمنطقة ما لن تسمح باستخدام استراتيجيات عسكرية عنيفة مثل ما هو الحال مع استراتيجية الصدمة والرعب (Shock and awe) التي تستخدمها الولايات المتحدة الأمريكية؛ يمكن النظر إلى أن الحرب الإلكترونية، وبالرغم أنها يمكن أن تحدث أضرار على مستوى قاري، وعالمي، مثل ما كان سيحصل في إيران، إلا انه يمكن القول أن الحرب الإلكترونية تتوجه أكثر إلى طرح الضربات الجراحية الدقيقة (Surgical strike)، بطريقة سرية، وباقل الأضرار الممكنة، وبأقل نسبة ممكنة من الانعكاسات السلبية على بقية الدول.

إن الاستعمال العسكري للتقانة يعد بمثابة سلوك طبيعي، وليس شاذ، وقد ذكرنا رأي هوكينج حين قال:[104]

" أعتقد أنه يجب اعتبار الفيروسات الحاسوبية وكأنها حياة(حياة). أعتقد أن هذا يعطينا نظرة عن الطبيعة البشرية إذ أن الشكل الوحيد من الحياة التي قمنا بخلقها (إنشائها) حتى الآن هي وإلى حد بعيد مُدمِرة بحتة. لقد قمنا بخلق شيء على صورتنا."

لهذا هناك من يتعامل مع الحرب الإلكترونية على أنها امتداد طبيعي لما تمثله الطبيعة البشرية، وجزء من عالم متغير يجب التأقلم معه، الأمر الذي سيجعل من التعاطي مع هذه الظاهرة الجديدة أمرا يجب القيام به من أجل توضيح، وتحديد المفاهيم المعتمدة عند التعامل مع قضايا الحرب الإلكترونية. إن

---

(104) Stephan Hawking, "British Physicist Says Computer Viruses Should Be Considered as a Life Form," ***the Daily News***, No 116, volume 23, Aug, 1994, p. 16.

- الحرب الشبكية(Netwar): مفهوم جديد لم تتم قولبته بعد بشكل جيد، له علاقة بالفواعل الغير رسمية في العلاقات الدولية، وقدراتها المتزايدة في التأثير عبر استخدام الشبكة لتحقيق مصالحها.

التعاطي مع الحرب الإلكترونية كمفهوم محدد ودقيق يعد صعبا نوعا ما، خاصة أنه هناك العديد من الأشخاص الذين يقومون بالخلط بين الحرب الإلكترونية، والحرب المعلوماتية، والحرب *الشبكية(Netwar)، [105] بل وحتى هناك من يربط الحرب الإلكترونية بالفواعل الرسمية فقط في العلاقات الدولية، وهذا ما عبر عليه المستشار في الأمن الإلكتروني في عهد الرئيس الأمريكي السابق جورج بوش(G.W Bush) ، ريتشارد كلارك (Richard A. Clarke) حين عرف الحرب الإلكترونية على أنها:[106]

"**هو ذلك الفعل، عندما تقوم الدولة القومية باختراق حواسيب دولة أخرى، وذلك من أجل إلحاق الضرر، أو تحقيق الاضطراب.**"

كما هناك أيضا من يرى أن الحرب الإلكترونية لا تعبر عن شيء واحد فقط، بل تدرس أربعة قضايا مهمة تتعلق بالجريمة الإلكترونية (cyber crime)، والتي يعبر عنها على أنها ارتكاب لجريمة ما عبر استخدام تقانة المعلومات، وهذا المفهوم يستخدمه خاصة رجال الأمن والقانون. ثم لدينا المجرمين الإلكترونيين (Cyber criminals)، والذي هدفهم الأساسي هو تحدي الأنظمة الأمنية من اجل تحقيق الذات، أو الشهرة، أو أية مصالح اقتصادية. بالإضافة إلى هذا يمكننا أن نجد الجوسسة الإلكترونية (Cyber espionage)، والتي تستخدم في الغالب، من اجل كسب مصالح سياسية أو عسكرية، فالتجسس الإلكتروني أمر منتشر جدا حاليا، وهو عنصر مؤثرا جدا، خاصة في المجتمعات المتطورة إلكترونيا، ونفس الأمر ينطبق على الإرهاب الإلكتروني (Cyber terrorism) الذي غالبا ما تكون لديه أجندة سياسية، وأيديولوجية يريد تحقيقها عبر استخدام مختلف الطرق السابقة التي تم ذكرها، وهناك أيضا من يعتبر هاكتفيزم (Hacktivism) الذي يعبر على نشاط سياسيين الذي يستخدمون الشبكة

---

[105] Serge S. Azarov, Alexander G. Dodonov, "Instrumental Corrections for a Definition of Cyberwar," in **NATO Security through Science Series - D: Information and Communication Security**, edited by Fernando Duarte Carvalho, Eduardo Mateus da Silva, (Published by IOS Press Online, Volume 4, 2006), pp. 3-24.

[106] Richard A. Clarke, Robert K. Knake, **Cyber War the Next Threat to National Security and What to do about it** (The United States of America: Ney York, published by Ecco, the first edition, 2011), p. 10

• الفرق بين كلمة (War)، وكلمة (Warfare)؛ هو أن (War) تعبر على فعل الحرب في حد ذاته، بينما (Warfare) تعبر على أساليب الحرب.

لتحقيق أهداف مختلفة.[107] وفي الأخير هناك ميدان الحرب السبرانية (Cyberwarfare)، هناك العديد من المفاهيم التي تعبر على هذا المصطلح، ولا يوجد الكثير منها التي تتوفر على الدقة والشمولية، وأفضل التعريفات التي قدمت هي التعريف الذي قدمناه سالفا لـ **ريتشارد كلارك**.

بالإضافة إلى ما سبق، هنا من القانونيين من يرى أن عمل الحرب الإلكترونية يتقارب من الناحية القانونية من إشاعة الرعب والإرهاب، لذلك هناك من يعرفها استنادا إلى هذه النظرة القانونية، حتى وإن كانت النظرة القانونية، وخاصة في القوانين الدولية تعد غير كاملة، وتعاني نقص كبيرا فيما يخص طريقة تصنيف الأسلحة الإلكترونية، ولهذا تجد أن الطرح القانوني هنا يرى الحرب الإلكترونية على أنها:[108]

> "**نظام قائم على الرعب المنتشر في الشبكة العنكبوتية، والتي تهدف إلى تنفيذ العديد من العمال لترويع أمن الأفراد والجماعات والمؤسسات والدول، وإرهاقهم اقتصاديا، وإدخالهم في أزمات نفسية واجتماعية ناتجة عما يعرف بالإرهاب الصامت.**""

يبدو من الواضح الآن أن الحرب الإلكترونية هي امتداد فعلي للوسائل التقليدية التي تعتمد في الحروب، ولهذا يمكننا أن نقر بوجود أليات عامة تحكم طبيعة الحرب الإلكترونية والتي من شأنها أن تقوم بالدفاع، أو بالهجوم على أهداف معينة، ولهذا يمكننا أن نقسم الحرب الإلكترونية عملياتيا إلى:[109]

1. عمليات الدفاع الإلكتروني:

وتشمل مختلف الإجراءات، والاستراتيجيات، والعمليات، والوسائل الدفاعية، وذلك من اجل إيقاف الخصم، أو التقليل من حدة الهجمات، وتتمثل هذه العمليات الدفاعية في عمليات للمنع، والوقاية من الهجمات المحتملة، والتحذير والتنبيه وفق قوانين الاشتباك

---

[107] Nicholas C. Ruster, ***The cybersecurity Dilemma***, Master's Thesis, not published (Duke University: Department of Political Science, 2011), p. 8-10.

[108] عياد سامي، ***استخدام تكنولوجيا المعلومات في مكافحة الإرهاب*** (مصر: الإسكندرية، نشر من قبل دار الفكر الجامعي، 2007)، ص. 65.

[109] سلامة صفات، ***اسلحة حروب المستقبل بين الخيال والواقع*** (أبوظبي: نشر من قبل المركز الإماراتي للدراسات والبحوث الاستراتيجية، الطبعة الأولى، 2005.)، ص ص. 38-39.

التقليديـــة، وكشـــف الثغـــرات والاختراقـــات الرقميـــة قبـــل حـــدوثها، أو معالجتهـــا بعـــد حـــدوثها، ووضع استراتيجيات استباقية لمنع تسرب أي معلومات محتملة.

2. عمليات الهجوم الإلكتروني:

تنطلـق معظـم الهجمـات الإلكترونيـة مـن قواعـد بيانـات، وأنظمـة خاصـة تقـوم عليهـا معظـم العمليـات التـي تـدخل فـي إطـار الحـرب الإلكترونيـة، وهـي عمليـات تهـدف إلـى السـيطرة علـى معلومـات الخصـم، لمنعـه مـن القيـام بـاي عمليـات يمكـن أن تسـبب الضـرر، حيـث يـتم التركيـز علـى ضـرب معلومـات الخصـم السياسـية، والاقتصـادية، والعسـكرية، مـن اجـل إلحـاق الضرر المادي والمعنوي.

يمكننـا أن نـرى هنـا أن الحـرب الإلكترونيـة تمتـاز بشـموليتها فـي تغطيـة مختلـف القطاعـات الحيويـة، ويمكـن أن تشـارك فيهـا مختلـف الفواعـل الموجـودة فـي العلاقـات الدوليـة، الرسـمية منهـا والغيـر رسـمية، فـالحرب الإلكترونيـة يمكـن أن تُعنـى بالعديـد مـن القطاعـات التـي يمكـن أن تكـون هدفا مهما لأي عملية افتراضية، ويمكننا أن نذكر بعضا منها وهي:

1. قطاع الاتصالات والمعلومات:

ولـــه علاقـــة بعمـــل جميـــع الشـــبكات التـــي يعتمـــد عليهـــا الاتصـــال داخـــل الـــبلاد، وعلـــى راســـها الشـــبكة العالميـــة، والحواســـيب، والشـــبكات الحكوميـــة، والمدنيـــة، والأكاديميـــة، والتجاريـــة، والخاصـــة، والمحليـــة، والخارجيـــة، ومحطـــات البـــث المرئيـــة، ومراكـــز الإشـــارات اللاســـلكية، وجميـــع الأنظمـــة التـــي يمكـــن إدراجهـــا فـــي خانـــة القطـــاع الاتصـــالية والمعلومـــاتي، فقطـــاع المعلومـــات يعـــد اكـــر القطاعـــات اســـتهدافا وتـــأثرا بـــالحرب الإلكترونيـــة كونـــه يحـــوي العديـــد مـــن الجوانـــب الحساســـة للدولـــة، والعديـــد مـــن الأنظمة التي لها علاقة وطيدة بالبنى التحتية للدولة. [110]

[110] البداية ذياب، ***الأمن وحرب المعلومات*** (عمان: نشر من طرف دار الشروق للنشر والتوزيع، الطبعة الأولى، 2006) ، ص. 36.

2. قطاع الأعمال العسكرية والحربية:[111]

ويتعلق بكل ما له علاقة بالتكنولوجيات التي يتم اعتمادها في العميات العسكرية، أو من حيث الإعداد اللوجيستي، ومن حيث الوظائف الإلكتروني للمعدات القتالية مثل ما هو الحال مع التشويش الإلكتروني للصواري جو–جو، أو لأنظمة الدفاع الجوي التي تعتمد على موجات الراديو من أجل تحديد أهدافها، إلى بقة الأنظمة التي أصبح يعتمد عليها حاليا من اجل القيادة عن بعد مثل الطائرات بدون طير، أو الاعتماد على الأقمار الصناعية من اجل تحديد الأهداف للصواريخ الجوالة.

3. قطاع الأعمال والأنظمة الحكومية:

يمكننا أن نرى حاليا انتشار ما يسمى بالحكومة الإلكترونية، ففي ظل الرقمنة المتزايدة، وحوسبة المرافق الحكومية، أصبحت الأهداف الحكومية، معرضة للخطر بشكل أكبر، ويمكننا أن نرى ذلك في الهجمات التي تقوم بها أنونيموس، على عدة مرافق حكومية أمريكية، للاحتجاج مثلا على سياسة معينة، كما يمكن أيضا أن تكون للعملية أبعاد أكبر عبر الهجوم على مواقع اقتصادية خاصة بعمل البورصات، أو البنوك، الأمر الذي يمكن أن يؤدي إلى نتائج كارثية في حالة لم تكن هناك خطة أمان للتعامل مع الأمر بشكل سريع. [112]

4. قطاع الطاقة والتوزيع الفيزيائي:

يمكن النظر إلى القطاعات الفيزيائية على أنها مجموعة البنى التحتية التي تضم القطاعات الهامة داخل الدولية، مثل ما هو الحال مع الأمن الوطني، والاقتصادي السياسي، والقضايا التي تتعلق بالمواصلات، والمراكز المسؤولة عن تسيير حركات النقل التي تعتمد على الأنظمة الإلكترونية، بالإضافة إلى هذا، يمكن إضافة القاطعات المسؤولة عن توليد الطاقة، والصناعات الثقيلة، والأساسية داخل الدولة. [113]

---

[111] وليد غسان سعيد جلعود، **دور الحرب الإلكترونية في الصراع العربي الإسرائيلي**، مذكرة ماستر، غير منشورة (جامعة النجاح الوطنية: كلية الدراسات العليا، 2013.)، ص ص. 91–92.

[112] كلارك ريتشارد، نيك روبرتة، **حماية الفضاء الإلكتروني في مجلس التعاون الخليجي** (أبوظبي: نشر من طرف المركز الإماراتي للدراسات والبحوث الاستراتيجية، الطبعة الأولى، 2011)، ص ص. 31–32.

[113] البداينة ذياب، ***مرجع سابق***، ص. 39.

5. قطاع المعلومات الإعلامية والمجتمعية:[114]

لا أحد يمكنه أن ينكر حاليا مدى أهمية وسائل الإعلام في السيطرة على الشعوب والأمم، وسنجد انه حتى في الحروب التقليدية، من بين أول الأشياء التي تقوم بها الدولة المستعمرة، هي تدمير وسائل الإعلام، كي تتوقف الدعاية، أو يتم توجيه الدعاية بطريقة تخدم مصالح جهة معينة، خاصة وأن الإعلام يعمل كمؤثر نفسي، في حالات الصراع، والسيطرة عليه يمكن أن يؤدي في العديد من الحالات إلى الحسم في الحرب الإعلامية (Media War).

6. قطاعات الاقتصاد والمال:[115]

تعيش الدول المتقدمة، والدول التي تحاول الصعود باقتصادها اليوم، مرحلة تحول حقيقية إلى اقتصاديات رقمية التي تتركز على مدى السيطرة على عنصر المعرفة المعلوماتية، وهنا تقع المشكلة، إذ هذا النوع من الاقتصاد القائم على التقانة، وشبكات الاتصال، وغيرها من أساليب التواصل الرقمي، بالإضافة إلى البورصات، والصكوك المالية الإلكترونية، والإنتاج الرقمي، والسلع الرقمية، والتجارة الرقمية، وكل أشكال النشاط الاقتصادي الموجودة على الشبكة؛ جعل من هذا المجال، أحد أكبر الأهداف الإلكترونية في الحروب الإلكترونية.

إن القطاعات المذكورة تختلف أهميتها من حيث اختلاف أوليات الدولة، فالدولة التي تعتمد على الاقتصاد الريعي ليست مثل الدول التي لديها اقتصاد متنوع، كما أن الدولة التي لها بنى تحتية إلكترونية، ليست مثل دولة لا بنى تحتية إلكترونية لديها، كذلك هو الأمر مع التعامل في البورصة، أو الانتخابات الإلكترونية، فالأمر دائما سيتوقف على تقدير الدولة الذي تريد الهجوم على الهدف، إذ لا فائدة مثلا من الهجوم على بنوك دولة تعتمد النموذج المركزي والتقليدي دي في دفع الأموال، أو نقل السندات، عكس الدولة التي تعتمد على بطاقات الدفع المسبق الإلكترونية.

بعد معالجة القطاعات، والأهداف التي يمكن أن توجه ضدها الحرب الإلكترونية، يمكننا الآن التعاطي مع الأسلحة الإلكتروني، أي الوسائل التي يتم اعتمادها في ظل الحرب

---

[114] وليد غسان سعيد جلعود، ***مرجع سابق***، ص ص. 94-95.

[115] المكان نفسه.

الإلكترونية، يجب أن نعرف هنا أنه لا يمكن التكلم على كامل الوسائل كونها عديدة جدا، ولكن عوض ذلك يمكننا تبويب هذه الوسائل من حيث الوظائف التي تقوم بها، مثل أن نصنف عدة أشكال من الأسلحة على أنها أسلحة بيضاء؛ فالأسلحة الإلكترونية لها نفس السياق، هناك استراتيجيات عامة يتم استخدامها، ولكن بطرق، ووسائل، وأدوات مختلفة، تتوافق كما، وعددا، ونوعا مع إمكانيات كل طرف، ووفق ما سبق يمكننا عرض هذه الوسائل وفقا لما يلي:

1. روبوتات إلكترونية(Botnets):

كما سنرى فيما بعد في حالة إستونيا، يمثل البوت نت أحد أشكال الهجمات الإلكترونية، وهو يعرف على أنه مجموعة من الحواسيب المربوطة ببعضها البعض بسبب وجود روبوت إلكتروني على حواسيبهم، الأمر الذي سيسمح لجهة معينة بالسيطرة على هذه الحواسيب التي يمكن أن يصل عددها إلى الملايين، والقيام بهجمات أخرى انطلاقا من هذه الحواسيب بطريقة واسعة جدا،[116] كما أن صاحب الحاسوب لن تكون له أي دراية بأنه يقوم بهذه الهجمات.[117] وهناك من يرى البوت نت على أنه عملية ربط مجموعة من الحواسيب بمتحكم واحد، وذلك من أجل سرقة الموارد الحاسوبية والشبكية بطريقة خفية وقابلة للنكر،[118] يعد هذا النوع من الهجمات، أحد أكثر الوسائل انتشارا في العالم حاليا،[119] وله علاقة وطيدة بهجمات حجب الخدمة.[120]

2. هجوم حجب الخدمة (Denial of Service):

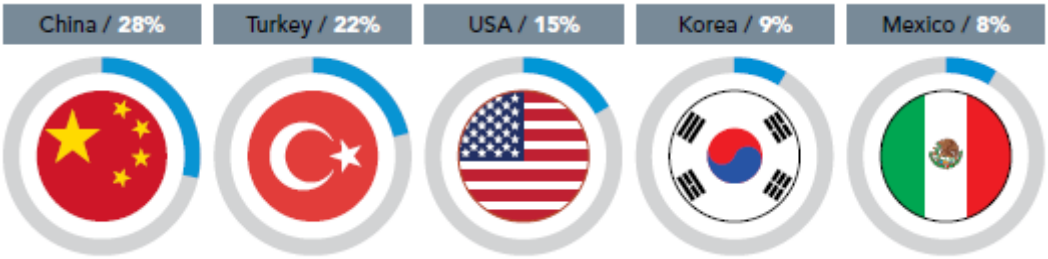
احد أبرز الهجمات الإلكترونية في العصر الحالي، وهجمات حجب الخدمة يمكن شرحها، عبر وجود فائض كبير في طلب الخدمة من نظام معين، الأمر الذي سيؤدي بالنظام، أو الملقم، أو الموقع، إلى السقوط، بسبب عدم قدرته على تلبية هذا العدد الهائل من الطلبات؛ الأمر بسيط لدرجة أن أي شخص يمكنه القيام بذلك بدون استخدام أي برنامج، لكن طبعا قيام شخص واحد فقط بذلك لن ينفع،[121] لهذا هناك طريقتين للقيام بعملية ناجحة، الطريقة

---

(116) Shane Harris, ***@War, The Rise of the Internet Military Complex*** (The United States of America, New York, Published by the Library of Congress, The first edition, 2014.), pp. 135-145.
(117) Julie E, Mehan, ***op. cit***, p. 132.
(118) P.W Singer, Allan Friedman, ***op. cit***, p. 294.
(119) Tatiana Tropina, Cormac Callanan, ***op. cit***, p. 5.
(120) Richard A. Clarke, Robert K. Knake, ***op. cit***, p. 131.
(121) P.W Singer, Allan Friedman, ***op. cit***, p. 295.

الأولى هو تضامن مجموعة من الناس من أجل القيام بهجمات على سلم عالمي ضد أهداف معينة مثل ما حدث في مهمة ضد إسرائيل (OpIsrael) بسبب قطاع غزة الأمر، الطريقة الثانية هي استخدام البوت نت وبينا سابقا من اجل تحرير الملايين من الأوامر في الثانية ضد أهداف محددة، ولهذا نجد أنه في الغالب تكون هذه الهجمات أكبر في الدول التي توفر خدمات عالية الأنترنت، كون العملية تحتاج إلى نسبة كبيرة من التدفق.

الصورة رقم: 1.3



5 أكبر مصادر لهجمات حجب الخدمة في العالم وفقا لتقرير الذي نشر سنة 2015

من قبل الشركة الأمريكية المتخصصة في الشبكات الإلكترونية أكماي (Akamai).[122]

3. قنبلة المنطق (Logic bomb):

وتسمى منطقية لأنها تتمثل في أن يقوم برنامج حاسوبي، أو 'إرشادات إلكترونية معينة، بإعطاء مجموعة من الأوامر المنطقية للحاسوب أو للنظام أو شبكة، من اجل أن يتم حذف كل البيانات الموجودة. وتعد هذه الطريقة في إلحاق الضرر خطيرة جدا، ويمكن أن نجدها مضبوطة مع ما يسمى الرد عند التحذير (Launch on Warning)، كآلية للرد الفوري عن وجود خطر على الدولة، أو أي جهة أخرى؛ فهذا الهجوم يعتبر كنوع من الإتلاف والتدمير الإلكتروني (Sabotage)، فلو قامت الصين مثلا بزراعة هذه الأوامر والبرمجيات الحاسوبية في الهياكل الأمريكية التي تتعلق بحصد المعلومات وتخزين وتوزيع المعلومات فإن النتائج ستكون عبارة عن تراجع كبيرة للقوة الأمريكية، خاصة وأن الولايات المتحدة الأمريكية تعتمد كثيرا على هذا الجانب.[123]

---

[122] Akamai's, **[state of the internet] Q4 executive review**, 2015, p. 8.
[123] Richard A. Clarke, Robert K. Knake, ***op. cit***, pp. 9-21.

4. الدود(Worms):

الدود الإلكتروني، هو عبارة عن برنامج يقوم بنسخ نفسه بطريقة سريعة، فطريقة عمل الدود تشبه طريقة عمل الفايروسات، [124] ولكن يمكن رؤية أن الاختلاف يمكن في قدرة الدود على إعادة خلق نفسه من أجل الانتشار، كم أيضا لدود ميزة في خلق الأبواب الخلفية، والأضرار التي يمكن أن يسببها يمكن أن تكون فائقة، بل وحتى تدمر مدن بكاملها كما سنرى في نموذج إيران، وفي نفس الوقت يمكنه أيضا أو يوفر الخدمة التي لها علاقة بحجب الخدمات الذي ذكرناها سابقا، وله دورا أيضا في التأثر على سرعة الشبكة، والانتشار عبر الشبكات أيضا. ولكن طبعا يجب معرفة، أن الدود ومدى قدرته لها علاقة بطريقة بتصميمه. [125]

5. الفايروسات(Viruses):

الفايروسات شبيهة لأحصنة طروادة من حيث الأهداف التي تهدف إليها، كونها تقوم على نفس القاعدة البرمجية، بالإضافة إلى هذا، يمكن للفايروسات أن تكون نائمة، أو مفعلة، أو يتم تفعليها عبر التدخل الإنساني، أو تبرمج على أن تفعل نفسها في زمن معين، فعكس الدود الذي ينتشر من تلقاء نفسه، يصعب للفايروسات الانتشار بدون تدخل إنساني، كون الفايروسات تكون في الغالب مدمجة مع ملفات. [126]

6. حصان طروادة (Trojan Horse):

يعمل حصان طروادة مثل الدود على البحث على الأبواب الخلفية في أي نظام من اجل استغلال الثغرات الموجودة فيه، كما أن الحصان يعمل كأنه برنامج عادي وذلك عبر تزييف نفسه للمستخدم، فالحصان عكس بقية الأسلحة، له وزن أكبر، ووظائف أكبر من الناحية العملياتية، رغم أنه يعتمد على عدة طرق مذكورة سابقا في الانتشار، رغم أن معظمها ليست ديناميكية وتحتاج إلى تدخل بشري لُتفَعل.

---

[124] Craig Smith, Ashraf Matrawy, Stanley Chow, Bassem Abdelaziz, "Computer Worms: Architectures, EvasionStrategies, and Detection Mechanisms," in ***Journal of Information Assurance and Security***, No 4(2009), pp. 69-83.

[125] Nicholas Weaver, Vern Paxson, Stuart, Robert Cunningham, "A Taxonomy of Computer Worms," in ***WORM***, No 3(October), 2003, pp, 1-8.

[126] Jeffrey Harton, Jennifer Seberry, "Computer Virusses an Introduction," in ***Computer Science Communications***, No 1, Vol 19(February, 1997), pp. 122-131.

يمكننا أن نرى هنا أنه هناك العديد من الوسائل من اجل القيام بالحرب الإلكتروني، والتي يمكن اعتمادها من طرف أبسط الأشخاص، ولكن يجب أن نعرف أن هذه الوسائل لا تعد نهائية، بل تمثل العناوين الكبيرة فقط، إذ يمكننا إيجاد العديد من الطرق الأخرى للصراع الإلكتروني، مثل التجسس المعلوماتي عبر استخدام الوسائل السالفة الذكر، والاختراق الإلكتروني، والقرصنة الإلكترونية، والرسائل الصامتة التي تعمل في الهواتف بطريقة سرية ولا يشعر بوصولها، وهناك من يضيف شبكات التواصل الاجتماعي والتي تعد افضل مكان لممارسة *الهندسة الاجتماعية، بالإضافة إلى مستوى آخر من القوة مثل الأقمار الصناعية، ودورها في جمع المعلومات، وما اصبح يسمى حاليا بالحقائب الكهروستاتيكية (Electrostatic Bag) التي لها نفس تأثير القنابل الكهرومغناطيسية، كما يمكننا أن نجد بعض الأسلحة التي تعد كأحد أشكال الحرب الإلكترونية مثل الطائرات بدون طيار، وقنابل التعتيم الميكروويفية (Blackout Bom) والتي لها نفس مفهوم الضربات الجراحية، ولكن ضد أهداف إلكترونية لجعلها خارجة عن الخدمة بدون تدميرها فيزيائيا. [127]

يمكننا أن نرى هنا أن الحروب الإلكترونية هي ميدان جديد، ولكنه في تطور متسارع ومستمر، فكل التكنولوجيات التي تم تطويرها من أجل السيطرة على العالم وبسط الهيمنة، وإلا وبرهن التاريخ على أنها ضعيفة وعرضة للاختراق والتلف، ويبدو أن هذا هو الشيء الذي تتميز به الحروب الإلكترونية، أو العالم الإلكتروني بشكل عام، فكل شيء معرض للخطر مهما كانت دفاعاته، ولا يمكن التكهن بمستقبل الحروب الإلكترونية، خاصة بسبب صعود جيل جديد متعلم، ومتأقلم مع التكنولوجيا، فإذا افترضنا أن العالم الذي نعيش فيه الآن يعد جديدا على هذا النوع من الحروب، فإن أ ي رؤية مستقبلية لمثل هذه الحروب، يجب أن تأخذ في الحسبان القاعدة الشعبية التي ستلج أكثر لتعلم هذه التقنيات. من البديهي أن نقول أن الحروب الإلكترونية، أو الأسلحة الإلكترونية، لا يمكنها أن تكون بمثابة الأسلحة النووية، إلا أنه يمكن للحروب الإلكترونية أن تسبب نفس الأثر الذي يمكن أن تسببه القنابل النووية، مثل هذه الأفكار تعطينا نظرة على عالم المستقبل، عالم تكون فيه الثقافة عالمية، واللغة الإلكترونية لغة عالمية، والحروب حروب عالمية، وأي شخص يمكن أن يكون جزءا من هذه الحرب.

---

[127] وليد غسان سعيد جلعود، ***مرجع سابق***، ص ص. 99-106.

- الهندسة الاجتماعية (Social Engineering): طريقة للقرصنة تقوم على دراسة الشخص بطريقة معمقة الأمر الذي يمكن أن يسمح بالتكهن بمعلومات الشخص، أو استخدام المعلومات التي تم جمعها، أو حتى معرفة الأرقام السرية لحسابات الشخص المستهدف.

1.4.1 الحرب المعلوماتية

مثل الحرب الإلكترونية، ينظر إلى حرب المعلومات على أنها أحد أشكال الحروب اللامتماثلة (Asymmetric warfare)، وصنف في الجيل الرابع من أشكال الحروب (Fourth Generation Warfare)، فالحرب المعلوماتية مفهوم له علاقة بالعقيدة الأمريكية، إذ أن الحرب المعلوماتية لها علاقة أكثر بالحرص على تحقيق التفوق القتالي في الأرض مهما كانت الظروف، والحرب الإلكتروني، تتعلق الحرب المعلوماتية أكثر بالمعطيات التي لها علاقة بالعتاد القتالي، والتكنولوجيات التي يمكن أن تحدث تغيير في الأرض، رغم أنه يمكن أن نجد الأنظمة والاستراتيجية التي لها علاقة بالحرب الإلكترونية، فالحرب المعلوماتية تتعاطى أكثر من القضايا التي لها علاقة بتنقل المعلومات، مثل التشويش، وموجات الراديو، والشبكات، ونوعية المعلومات التي تنتقل أيضا، ويركز في العادة على القضايا الهامة من اجل سلامة الاستمرارية مثل عمل البورصة وطرق المواصلات، والطرح هنا شبيه بتامين مصادر الماء في الحروب القديمة، فهناك أمور حيوية يمكن أن تكون لها علاقة بالاقتصاد، أو الذكاء الصناعي للمعدات، ومقاربة الأمن المعلوماتي تهدف إلى توفير ذلك الغطاء الأمني.

الحرب المعلوماتية في طبيعتها هي حرب رقمية، وإلكترونية، ولها علاقة بحماية الموارد بمختلف أنواعها في ساحة الحرب، وفي نفس الوقت، العمل على كشف أي معلومات غير صحيحة يتم تداولها، أو الحرص على معلومات لا يجب تداولها أثناء العمليات القتالية، ويمكن عرض مجموعة من الفصائل التي تم إدراجها تحت مضلة الحرب المعلوماتية، ويمكن ذكرها وفقا لما يلي:[128]

1. أمن العمليات (operational security).
2. الحرب الإلكترونية (electronic warfare).
3. العمليات النفسية (psychological operations).
4. الخداع (deception).
5. الهجوم الفيزيائي على معالجات المعلومات (physical attack on information processes).
6. عمليات الهجوم المعلوماتي (information attack on information processes).

---

[128] Brian Nichiporuk, " U.S Military Opportunities Warfare Concepts of Operation," in ***United States Air and Space Power in the 21st Century***, edited by Zalmay Khalizad, Jeremy Shpiro (The United States of America: published by RAND, 2002), pp. 187-220.

يمكننا أن نرى التنوع في الآليات والحقو التي تهتم بها الحرب المعلوماتية، فالحرب المعلوماتية تهدف بشكل أساسي إلى التفوق المعلوماتي في أرض القتال، وهذا الأمر يمكننا رؤية في التعريف التالي للحرب المعلوماتية والذي ينص على أن الحرب المعلوماتية هي:[129]

> "**الأفعال والإجراءات التي يتم اتخاذها من أجل تحقيق التفوق المعلوماتي، عبر التأثير على معلومات العدو، ومراكز معالجة المعلومات، وأنظمة المعلومات، والشبكات الحاسوبية مع الدفاع المستمر على المعلومات الشخصية، ومراكز معالجة البيانات، وأنظمة المعلومات، والشبكات الحاسوبية**".

كما أن التطرق إلى الحرب المعلوماتية، ومثلها مثل باقي المفاهيم المتعلق بالحرب الإلكترونية، هناك العديد من الضبابية حول المفهوم، إذ يمكن إيجاد أنه حتى في القيادات العسكرية الأمريكية، والتي

تعد بمثابة البيدق في تطوير هذا المفهوم، إلا انه لديها تفاسير مختلفة إذا ما سأل مختلف الأشخاص في القيادة العسكرية، فهناك من يربط الحرب المعلوماتية بالتشويش والخداع (Jamming and Spoofing)، وهناك من يربطها بشكل خاص بالقيادة الحربية (Command and Control Warfare)، يمكن فهم هذه الاختلافات ربما عبر الاطلاع على رتب الأشخاص، ولكن يرى أن متغير المعلومات، دائما حاضر في الحرب المعلوماتية، إنها المعلومات التي لها علاقة مباشرة بالتفوق القتالي على الأرض. [130]

تعد الحرب المعلوماتية أحد الوسائل الهيمنة العالمية، فالمعلومة أصبحت لها قيمة أكبر في هذا العصر، كونها أصبحت تشكل قيمة مادية في حد ذاتها، فقد أصبحنا الآن في عالم أين أصبح الضرر التي يُتسبب للمعلومات، يترجم، بأضرار فعلية لأرض الواقع، بالإضافة إلى هذا يمكننا أن نقول أن ميدان الحرب المعلوماتية، وحتى لو له العديد من مزايا الحرب الإلكترونية، إلا انه يمكننا القول أنه موجه أكثر للاختصاص العسكري ذو السلم الواسع، ذلك أن التقانة المستخدمة مثل ما هو الحال مع تكنولوجيات

---

[129] Reto E. Haeni, "Information Warfare an introduction," in: ***http://goo.gl/FCnKcN***, (Wednesday, May 11, 2016).

[130] Roger C. Molander, Andrew S. Riddile, Peter A. Wilson, **Strategic Information Warfare, A new Face of War** (The Unites States of America: published by RAND, 1996.), p. 1.

التشويش التي تعد متقدمة جدا وتحتاج لموارد مالية كبيرة جدا من أجل تصنيعها، الأمر الذي لا يمكن لمواطن واحد أن يحققه، ولكن يمكنه عوض ذلك التأثير على هذا النوع من التكنولوجيات عبر قرصنتها.

1.4.2 الحرب التشفيرية

لقد تكلمنا من قبل على التشفير، وأهمية التشفير من أجل حماية البيانات؛ لكن تطور وسائل جديدة لتعمية وإخفاء البيانات، جعل العديد من الحكومات ترى ذلك على أنه تهديد جديد يجب القضاء عليه، أو الحد من توفر وسائل متقدمة لتشفير البيانات للعامة، بطريقة تجعل السلطات المعنية لها القدرة على فك التشفير متى هي أرادت ذلك، هذه المعضلة بدأت تطرح نفسها مع بداية التساؤل حول بداية انتشار الأنترنت، وبروز العديد من التخوفات حيال القضايا التي تتعلق بالخصوصية، وتسرب المعلومات، والتجسس الحكومي على المواطنين، وتجسس دول على دول أخرى، فالحرب التشفيرية(Crypto Wars)، وقضايا التشفير أصبحت لها أهمية كبيرة في الحياة الإنسانية، كون أن الشخص، ومثل ما كان يحرص على خصوصيته، هو الآن يعمل جاهدا، من أجل تحقيقها في هذا العالم المعولم.

إذا كان التشفير يعد شيء جديد بالنسبة للمواطن العادي خاصة مع بروز الأنترنت، فالأمر لا يعد جديدا للباحثين المتخصصين في الشبكات الإلكترونية، وتنقل المعلومات؛ وهذا ما يمكننا أن نراه فعلا، إذ أن اهم وسيلة للتشفير، والتي يتم اعتماها حاليا من قبل الجميع، هي تقنية التشفير أر.أس.أي (RSA)، تستعمل هذه التقنية لأنها مفتوحة المصدر، ويمكن لأي شخص اعتمادها، واسم هذه التقنية يشير إلى أسماء ثلاثة باحثين عملوا عليها، وقاموا بتطويرها، فقد قام كل من العالم الإسرائيلي في التشفير **عدي شامير** (Adi Shamir)، والمشفر **رون ريفست** (Ron Rivest)، وعالم الحاسوب **ليوناردو أدلمان** (Leonard Adleman)؛ بتطوير نظام خوارزمي يسمح بتشفير الملفات، وقد اصبح هذا النظام يستخدم حاليا بشكل واسع، فمعظم الموقع أو الشركات حاليا تستخدم تشفير يعتمد على مفتاح 1024 بيت من اجل تامين البيانات المخزنة، والبيانات المتنقلة الذي يتبادلها المستخدم مع المواقع مثلا.[131]

[131] Sara Robinson, "**Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders,"** in ***SIAM News***, No 5, Volume 36(June, 2003), pp. 1-4.

ولكن هناك العديد من الشركات الكبرى حاليا التي رفعت مستوى الدفاع لديها إلى 2048 بيت، [132] وهو ما يعادل 617 رقم، وقد كان هذا التحول خاصة بعد التسريبات التي قام بها إدوارد سنودن (Edward Joseph Snowden) سنة 2013، وخاصة تلك التي تتعلق ببرنامج بالران (Bullrun)، فقد كان يعمل هذا البرنامج على فك، وتكسير التشفير على نطاق واسع للمفاتيح الموجودة على الشبكة، [133] كما العمل على إدراج ما يسمى بالأبواب الخلفية(Backdoors). [134]

لقد كانت هناك ردود أفعال كبيرة على التسريبات، إلى درجة أن ألمانيا قامت بفك عقد كان يربطها بالولايات المتحدة الأمريكية، وبريطانيا، في القضايا التي تتعلق بالتعاون في المجال الاستخبارات والتجسس، كل هذه الأحداث تدفعنا إلى تفهم رغبة الناس في الخصوصية، خاصة أثناء التواصل، ويمكننا أن نرى ذلك عبر تضاعف استخدام لشبكات تور البصلية. [135]

يمكننا فهم الحرب التشفيرية عبر المطالب الذي تريدها بعض الحكومات، مثل ما هو الحال مع الولايات المتحدة الأمريكية، وبريطانيا، فالأبواب الخلفية التي ذكرناها سابقا، يمكن شرحها خارج نطاق عالم التشفير، على أنها الأبواب الخلفية لأي برنامج، يقوم المبرج بصنعها، كي يتمكن من الدخول إلى البرنامج فيما بعد، من أجل الصيانة أو التحديث، أما في عالم التشفير، فالأبواب الخلفية بالنظرة التي تسعى إليها بعض الدول؛ هي تقنين عملية التشفير بطريقة تكون هناك أبواب خلفية، والتي فقط سلطات حكومية معينة لها الحق الولوج إليها، والدخول إلى أي جهاز مشفر مسبقا، وقد ذهب الأمر حتى إلى إعلان بعض الدول مثل بريطانيا، عن نيتها في اعتبرا التشفير المتقدم أمرا غير قانوني.[136]

يمكننا فهم هذا التخبط الذي تعاني منه بعض الدول، مثل الولايات المتحدة الأمريكية، بسبب القوانين التي تتعلق بالحرية الشخصية، والتي تتعارض مع إجبار شخص على إعطاء مفتاح التشفير،

---

[132] Michael Mimoso, "Google Completes Upgrade of its SSL Certificates to 2048-Bit RSA," in: ***Https://goo.gl/zFCoc8***, (Tuesday, May 03, 2016).
[133] Jeff Larson, "The NSA's Secret Campaign to Crack, Undermine Internet Security," in: ***https://goo.gl/vm2VSJ***, (Tuesday, May 03, 2016).
[134] James Ball, Julian Borger, Glenn Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security," in: ***http://goo.gl/8FrMwd***, (Tuesday, May 03, 2016).
[135] Douglas Wikstrom, "A universally composable mix-net," In ***Theory of Cryptography Conference (TCC)***, Volume 1(2004), pp. 317-335.
[136] Jane Wakefield, "Can the government ban encryption," in: ***http://goo.gl/irV6cu***, (Tuesday, May 03, 2016).

ويمكننا أن نرى ذلك مثلا في الدستور الأمريكي، في التعديل الخامس، حيث يعالج جزء منه هذه القضية بطريقة غير مباشرة، وذلك حين يعبر على أنه :[137]

"... **لا أحد يمكنه، في قضية جنائية، أن يُجبر على الشهادة ضد نفسه ...**"

ويمكننا أن نفهم هنا، أنه حتى لو طلبت السلطات من أي شخص إعطاء المفتاح من أجل تحقيق معين، فإنه لديه الحق في الرفض، مستدلا بهذا القانون الذي يعطيه الحق في رفض البوح باي معلومة، أو إعطاء مفاتيح فك التشفير، وهناك العديد من القضايا الجنائية التي حدثت في الولايات المتحدة الأمريكية، والتي كان المتهم فيها ضالع بقضايا تتعلق بالغلمانية (Pedophilia)، لكنه رفض إعطاء المفاتيح للأقراص الصلبة التي كان يخزن بها البيانات بسبب القانون المذكور سالفا. [138]

لكن الأمر لا يتوقف هنا، إذ هناك العديد من الحالات، والتي تطلب فيها حكومة أي دولة، معلومات من شركة معينة لفك تشفير هاتف معين مثلا، ولهذا بدأت العديد من الشركات مثل ما هو الحال مع شركة آبل(Apple)، وميغا(Mega)، العمل بما يسمى تشفير الند لند (End-to-end encryption)، بهذه الطريقة، حتى الشركة نفسها لن تقدر على إعطاء مفتاح التشفير الذي سيسمح لجهة معينة الولوج إلى البيانات ولو تحت ضغوطات قانونية، والسبب في ذلك يعود إلى أن الشركة نفسها لا تعرف المفتاح، فهذه التقنية في التشفير تسمح لشخصين بالتواصل، والشخصين فقط لديهما المفتاح، بهذه الطريقة تؤمن الشركة نفسها من المتابعة القانونية.[139]

من هنا، وفي ظل هذه المصاعب المتزايدة، هناك من يستعمل تقنية *هجوم الطاقة العمياء (Brute-force attack) من اجل العمل على فك أو تكسير الشفرات(Factorization)، الأمر الذي سيسمح بالولوج إلى أية معلومات مشفرة. هذه العملية تعد صعبة حاليا، خاصة إذا تعاملنا مع مفاتيح 2048 بيت، الأمر الذي يمكن أن يأخذ عمر الكون كله لتكسير الشفرة؛ هجوم الطاقة العمياء له علاقة

---

[137] United States Constitution, ***Fifth Amendment of the United States Constitution***, 1789.
[138] Joel Hruska, "US Appeals court upholds Fifth Amendment right to not decrypt hard drives," in: ***http://goo.gl/fVAAZt***, (Tuesday, May 03, 2016).
[139] Andy Greenberg, "Hacker Lexicon: What Is End-to-End Encryption?," in: ***https://goo.gl/HRw386***,(Tuesday, May 03, 2016).

- هجوم الطاقة العمياء (Brute-force attack): هجوم يستند غلى القدرة الحاسوبية، ويقوم على تجربة كافة الاحتمالات، حتى إيجاد المفتاح، فإذا كان طول المفتاح ثلاثة أرقام مثلا، فهذا يعني تجربة 999 احتمال حتى يجد المفتاح.

مباشرة بالقوة الحاسوبية، فكلما كان الحاسوب أقوى، كان ذلك أفضل، ففي ظل تزايد القوة الحسابية للمعالجات الحاسوبية كما يؤكده قانون مور، [140] بالإضافة إلى الثورة التي يمكن أن تحدثها الحواسيب الكمية، سيكون تكسير هذه المفاتيح المذكورة سهلا، لكن العالم سيذهب إلى مفاتيح أكبر طبعا من لمجاراة هذا التقدم.

ولكن الذي يهمنا هنا، هو الدور الذي أصبحت تلعبه حرب التشفير في المعادلة الدولية ومكافحة الهيمنة في العلاقات الدولية، لقد قلنا من قبل أن الهيمنة الإلكترونية، هي بمثابة امتداد طبيعي للمفاهيم التقليدية للهيمنة، فالحرب التشفيرية تخص أي شخص يعيش في القرن الحالي، ذلك أن أي واحد منا أصبح معني بهذه القضايا المشتركة؛ إذ يمكننا أن نرى هنا وجود وبروز وعي اجتماعي دولي حول المصالح المشتركة، وكيفية مكافحة هيمنة الدول، والسلطات، هذا الوعي المشترك الذي لا حدود له، أصبح يتقاسمه معظم سكان الأرض، الأمر الذي سمح بتشكيل أرضية متينة للقيم التي يجب أن تخدمها التقانة ، وهي قيم، وقضايا تتعلق بالحريات الشخصية، والخصوصية، وخدمة الإنسانية. فالحرب التشفيرية هي حرب مفتوحة لم يعلن من هو الفائز فيها بعد، وهي حرب يشارك فيها الجميع، بداية من المواطن البسيط، إلى المنظمات، إلى الدول، وهي أيضا حرب تعني الجميع، سواء أرادوا ذلك أم لا، فالحرب التشفيرية هي إحدى مؤشرات الهوية العالمية، وعولمة الأفكار، والمبادئ، وعكس العديد من القيم المنتشرة بسبب العولمة، تعد القيم التي خلقتها الحرب التشفيرية، قيم وليدة التقانة.

1.5 الرقمنة

يمكن التكلم على أن من بين أهم الأشياء التي ميزت الطفرة التقنية، والعلمية في العصر المعلوماتي، هي الفعل، أو تلك العملات، التي سمحت بتحويل العديد من الأشياء التي كانت تصنع واقعنا اليومي، إلى واقع افتراضي يمكن التعامل معه بطريقة مختلفة على التي كنتا نتعامل بها، لقد برزت الرقمنة (Digitizing) كعملة سمحت بتغيير نمط عيشنا اليوم، وذلك عبر تغيير جذري للعديد من الأفكار، والمسلمات التقليدية، مثل ما هو الحال مع التعامل مع الثروة، والممتلكات، والمعلومات، والسرية، والعلاقات الاجتماعية، والتواصل، والخدمات، والتعلم، والعديد من الأشياء التي تصنع الحياة اليوم لكل شخص، هذه العملية، ورغم أنها قد جاءت بالعديد من الفوائد المتزايدة، إلا أنها غيرت أيضا نظرة الناس

[140] ميتشيل والدروب، "ما بعد قانون مور،" ***الطبيعة***، العدد 44، (أبريل،2016)، ص ص. 32-35.

إلى الأمن، وإلى الطرق الجديدة لإلحاق الضرر، ويتبين هنا أنه من الواضح جدا أنه يجب تغيير طريقة التفكير، إلى طريقة أكثر ملائمة، إلى هذا الطرح اللامركزي للحياة الإنسانية، فالرقمنة، وكأي ظاهرة جديدة، قد احدث تغييرا جذريا في طريقة عيشنا، أكانت بطريقة إيجابية، أو سلبية، لكن المؤكد هنا، هو أنها عملية غير رجعية، وهي في تزايد، وإدراج مستمر في الحياة الإنسانية.

يمكن النظر إلى النجاح الذي حققته التقانة، كما دخولها إلى الحياة الشخصية للناس إلى ابعد الحدود، على أنها نتيجة المميزات التي وفرتها تكنولوجيات الإعلام ،والاتصال، والقدرة على تخزين البيانات، كما توفر تلك القدرة التي تسمح بحمل كافة ومختلفة المعلومات بطريقة فعالة، لهذا يمكن ننظر إلى الرقمنة على أنها عملية تحويل للقيم مهما كانت إلى قيمة افتراضية،[141] وكذلك إلى قيم ديناميكية، يمكن أن توظف داخل أنظمة مغلق أو مفتوحة، في إشارة إلى العتاد العسكري، والأقمار الصناعية، وكل ما له علاقة بالشبكات وتنقل المعلومات.

ويدخل الأمر في نفس سياق الحرب الرقمية، كون أي شيء تم رقمنته، هو عرضة للإتلاف أو القرصنة، أو السرقة، ففي العالم الرقمي، لا يمكن التكهن بالنتائج، إذ لا أحد لديها السيطرة الكاملة على ما يحدث في الشبكة، حتى الولايات المتحدة الأمريكية، والتي تعد اكبر قوة عسكرية، لم تتمكن من هذا المجال، خاصة وأن الخبار يؤكدون أن الحروب القادمة ستكون إلكترونية، وحتى الولايات المتحدة الأمريكية، والتي لها اكبر ميزانية عسكرية، تعد غير مؤهلة وجاهزة لذلك.[142] كذل يجب النظر إلى الجرب الرقمية بنفس النظرة التي ينظر بها إلى الإلكترونية، كونها تعد أحد أشكالها، ويمكن حتى أن تتعلق بالأنظمة الدفاعية العسكرية، والدور التي أصبحت تلعبه في الحروب والصراعات الحديثة كما حدث في سوريا مؤخرا فيما يخص أنظمة الدفاع الجوي.[143]

ولهذا، هناك من ينظر إلى الرقمنة، من زاوية النتائج الكارثية التي أحدثتها على المستوى السياسي، والدولي، والاجتماعي، خاصة تلك الأحداث التي تمثلت هجوم شامل من قبل دول على حكومات محددة، أو على الأنظمة الاقتصادية التي تعتمد عليها الدولة من أجل تسيير شؤونها الاقتصادية، مثل ما هو الحال مع التعاملات البنكية الإلكترونية، أو الإلقاء المرنائي، فمثل هذه العمليات، أو المخاطر، أصبحت

---

(141) Denis McQuail , ***Communication Theory*** (The United States of America: California, published by Saga Publication Inc, the first edition, 1983.), p. 40.
(142) David Stupples, "The Next Big War Will Be Digital—and We're Not Ready For It," in: ***http://goo.gl/SqujuL***, (Saturday, May 07, 2016).
(143) Edward Boxx, "Observations on the Air War in Syria," in ***Air & Space Power Journal***, (March–April, 2013), pp. 147-168.

تشكل هاجسا حقيقيا للدول من أجل ضمان امنها، وأمن المواطنين، ومصالحها الخارجية والداخلية، ويمكننا حتى أن نرى حاليا، وخاصة في مجال التنظير في العلاقات الدولية، أن الرقمنة، والأمن الرقمي، اصبح يتواجد أكثر فأكثر في حقل الدراسات الأمنية المعاصرة، ليس كفرع وإنما كعلم قائم بذاته،[144] الأمر الذي يوضح لنا فعليا الأهمية الكبيرة للرقمنة في الحياة السياسية حاليا، بل يمكن القول أنه قد أصبحت هناك العديد من الأشياء التي لم يعد بإمكانها الاستغناء عن التقانة، كونها أصبحت جزء من نظام عملها، كما التعود ورسم السياسات بناء على مخرجات تعتمد على السرعة الإلكترونية في التبادل، جعل من فشل أو أي انقطاع في هذا التواصل أمر خطيرا.

يمكن النظر إلى الرقمنة إلى تلك العملية البسيطة التي يمكنها أن تحول أي معطى مادي، أو معني، إلى معطيات وبيانات رقمية يمكن التعامل معها وفق كل المزايا التي توفرها الشبكة العالمية؛ لكن من جانب آخر على كل أن يأخذ بمبدأ التلفيق المعلوماتي (Disinformation) كهامش مقبول للضرر على أي مستوى يمكن تصوره، فهذه الحرب الخفية على التحكم هي ميدان الأقوياء، فقد صرح **صن تزو** على أن الحرب هي ميدان الحياة والموت، ويمكننا أن نقول أن نفس الفكرة تنطبق على الرقمنة وانعكاساتها على الإستراتيجية العسكرية ورؤية الدول للحروب وإلحاق الضرر، ويجب أن نقول أن هذا الضرر ليس نتاج عملية قصدية، ومخططة دائما كما سنرى لاحقا مع الانعكاسات الاجتماعية، والنفسية للرقمنة.

1.5.0 الجيومعلوماتية

تعبر الجيومعلوماتية على تحول جديد في إدراك الجغرافيا، وطريقة جديدة في تحديد طرق الهيمنة العالمية، فمما لا شك فيه، تعتبر الموارد الطبيعية، أحد اهم الأسباب التي يمكن أن تجعل منطقة معينة ذات أهمية جغرافية، كما تجسدت العديد من الطروحات والتي اعتمده على المعطيات المكانية كأحد أهم محددات السيطرة العالمية، أو البحث على الثروة، كذلك هو الطرح الذي ذهبت إليه الحتمية الجغرافية (Environmental determinism)، ومعظم

(144) Lene Hansen, Helen Nissenbaum, "**Digital Disaster, Cyber Security, and the Copenhagen School**", in International Studies Quarterly - International Studies Association, Volume 53, 2009, pp. 1155-1175.

نظريات السيطرة العالمية، مثل نظرية قلب العالم (eartland Theory) للجيوسياسي والجغرافي **هالفورد ماكيندر** (Halford John Mackinder 1861-1947) ، أو عند **الفريد ماهان** (Alfred Thayer Mahan 1840-1914) الذي تكلم على السيطرة على البحر، كما النظرة الأمريكية التي تتكلم على السيطرة على الهلال الخصيب؛ كل الطروحات التي ذكرناها هنا، وبغض النظر عن الأهداف السياسية، أو الأيديولوجية المعلنة، إلا أنه لها مرجعية مكانية قوية جدا، ولعل ذلك يعود في الغالب يعود إلى عدة أسباب، مثل طبيعة العقيدة العسكرية المنتشرة في كل فترة، كم نوع ومدى تطور التقانة في كل فترة، أو حتى المتطلبات الاقتصادية والاجتماعية لكل دولة، ولهذا سنجد حاليا أن الجيومعلوماتية، تمثل طرحا جديدا للسيطرة المكانية، وأهمية مناطق معينة على مناطق أخرى، هذه الأهمية، وحتى لو كانت تستند إلى بعض المعطيات الجغرافية المتعلقة بالسلامة، إلا أنها تستند بشكل اكبر على تدفق المعلومات، وتخزينها.

يمكن الظر إلى الجيومعلوماتية على أنها نوع جديد من المصالح، حيث أن العالم يتجه حاليا إلى تكوين تكتلات سياسية، أو عسكرية، هذه التكتلات لديها أبعاد ترتكز على المعلوماتية، والتكنولوجية، وتهتم الجيومعلوماتية أيضا بجمع وتحليل المعلومات، والأثر الذي يمكن أن تسببه الإستراتيجية المعلوماتية على الاستراتيجيات الوطنية على مختلف أشكالها.[145] لقد ساهم التطور على تغيير الحياة التي يعيشها الإنسان، ولكنه اهم من جانب آخر في طريقة تعامله مع التجارة، والسياسة، فالجيومعلوماتية وضعت قواعد لعبة جديدة تستند على السيطرة على عدة عوامل، مثل ما هو الحال مع السرعة، والتكنولوجيا المتقدمة، مثل هذا النوع من السيطرة، يمكن أن تكون له علاقة بالمعلومات المخزنة مثل ما بيننا سابقا مع قيام دول البريكس بإنشاء خط الأنترنت الخاص بها من أجل تخزين مركزي للمعلومات داخل الدولة، كما يمكن أن تكون له علاقة بنقاط تدفق المعلومات، ومدى سرعتها في الوصول إلى الأهداف المرجوة.

قضية السرعة يمكن فهمها عبر التطرق إلى ما أصبح يسمى حاليا بالتداول العالي التردد أو الفائق التردد (High-frequency Trading)، إذ أن هناك العديد من الشركات التي تسعى إلى أن يكون خط الأنترنت الذي يربطها بالبورصة أو الأقرب، إذ أن الشركة التي لها خط أسرع، يمكنها أن تعرف بالأوامر المرسلة من قبل أشخاص أو شركات، وبذلك ترسل أمر يصل بشكل أسرع من أوامر بعض الشركات أو

---

[145] وليدة ساعو، ***الثورات العربية بين التوازنات والتفاعلات الجيوستراتيجية ومتغيرات المنقطة العربية***، مذكرة الماستر، غير منشورة، الجزائر، بسكرة (جامعة محمد خيضر: كلية الحقوق والعلوم السياسية ، 2013.)، ص. 14.

الأشخاص، من اجل شرا الأسهم، بذلك فلما يرسل الشخص مثلا أمرا بشراء 30.000 سهم، فإن فرص حصوله على ثلث هذا العدد فقط تعد كبيرة، كون خط الاتصال الذي يعتمد عليه أطول في المسافة، أو اقل سرعة من الذي تعتمده شركة أخرى، الأمر الذي سيسمح لبعض الشركات بتضخيم أرباحهم، وذلك فقط لانهم الأسرع، ولهذا فالموقع الجغرافي أصبحت لديهم أهمية فائقة جدا، فائقة لدرجة أن بعض البورصات التي تقوم بإيجار غرف خاصة بالتداول، تقوم بحساب خط الأنترنت الذي يربطها بالبورصة بدقة ميليمترية من أجل المساوات بين الجميع الذي يستعملون هذه الغرف.[146]

يمكننا أن نرى في **الخريطة رقم 1.0** توضيحا للأهمية التي ذكرناها سابقا والتي تتعلق بالسرعة، ويمكننا أن نرى أن النقاط الحمراء، تعبر على أحد أهم منصات التداول في المنطقة، النقاط الزرقاء تعبر عن أفضل مسافة موجودة بين بورصتين تستخدمان التداول العالي التردد، وبذلك تكون سرعة الاستجابة أكثر بكثير، الأمر الذي دفع العديد من الخبراء إلى توقع أنه سيكون في المستقبل منصات على الماء، أو في قوارب خاصة، تكون مهمتها الخاصة هي ربط الاتصال، وإتمام عميات التداول الفائقة السرعة، كما حتى امتلاك الشركات الكبرى للتداول، شركات خاصة بها للربط الشبكي في ظاهرة جديدة أطلق عليها اسم الألياف السوداء (Dark fibre).

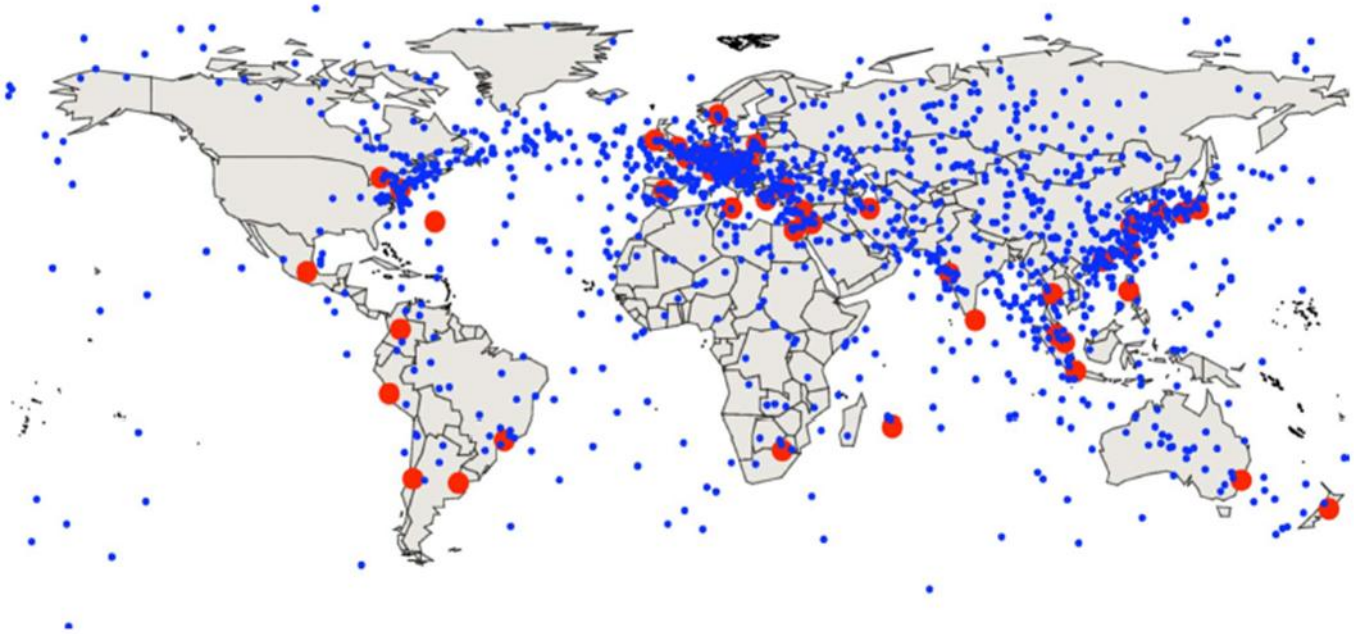
إذ نظرنا كيف للجيومعلوماتية أن تؤثر على اللعبة الدولية، أو العلاقات الدولية، أو حتى بسط الهيمنة الدولية، يمكننا النظر إلى ما أصبحت تمثله المعلومات في العلاقات السياسية، والاقتصادية، والعسكرية، فمثلا يمكننا أن نجد في مدينة بزيلدون (Basildon) في بريطانيا العديد من البورصات الأوروبية والأمريكية، إذ يمكننا أن نجد بورصة باريس، وأمستردام، وبروكسل، وليزبون، ولكسمبرغ، كل هذه البورصات تعمل في مكان واحد مؤمن أكثر من القواعد العسكرية، كما أن هذا المكان محمي حتى ضد سقوط الطائرات ، والانفجارات النووية؛ فهذا المكان يحوي ملقمات تعمل على خوارزميات لشراء الأسهم وبيعها، وبطبيعة الحال وفي نظر الجيومعلوماتية، يعد هذا المكان منطقة فائقة الأهمية، لا بسبب معطيات مكانية تتعلق بالجغرافيا أو الموارد، وإنما للأسباب تتعلق بالمعلومات الموجودة في المنطقة، ويمكننا هنا تصور أن الأضرار في حالة تم الهجوم على هذه المنطقة ، وتدمير المركب بطريقة المفاجئة يمكن حسابها على سلم عالمي.[147]

---

[146] مارك بوكنان، "التداول بسرعة الضوء،" ***الطبيعة***، العدد 31، (بريل، 2015)، ص ص. 39-41.

[147] Ivan Macaux, le Turbo Capitalisme, Nouveaux Loups de WallStreet, Documentaire, dans : ***https://youtu.be/vOzH7Aj2MOA***, (samedi 7 mai 2016).

الخريطة رقم: 1.0



شكل يوضح أهم المراكز المالية للتداول وتنقل المعلومات،

بالإضافة إلى أفضل المواقع للقيام بعمليات التداول. [148]

لقد غيرت التقانة وبطريقة جذرية طريقة رؤيتنا للقوة، وطريقة كسبنا للقوة، والجيومعلوماتية تعد نموذجا آخر للوجه الجديد لهذا العالم، لقد أصبحت المعلومات مصدرا للقوة، والسيطرة العالمية، وأي جهة تريد أن تصبح شريكا في اللعبة السياسة الدولية، يفترض بها أن توفر مستوى قاعدي من السيطرة على التكنولوجيات المتقدمة، ولكن كما رأينا، فإن الجيومعلوماتية، وخاصة إذا نظرنا إلى ما يعبر عليها من حيث الهياكل المادية، يمكننا أن نقول أنها تعد جد ضعيفة، وحساسة جدا، الأمر الذي يمكن أن يلعب لصالح جهات أخرى في ظل أي صراع من اجل القوة، والسيطرة، أو حتى فقط من قبل بعض الأشخاص عبر القرصنة الإلكترونية، أو الإتلاف المتعمد للأنظمة لأي سبب كان.

[148] A. D. Wissner Gross, C. E. Fre, "**Relativistic statistical arbitrage,**" in ***Physical Review – Electronic publishing E***, Volume 82, Issue 82, (November, 2010).

1.5.1 السايبرفوبيا

تمثل السايبرفوبيا (Cyberphobia) سلوكا اجتماعيا جديدا يتمثل في التخوف المستمر والدائم، بسبب عدم المعرفة أو عدم التمكن، من كل ما هو إلكتروني وشبكي. إن قضية التخوف من تسرب المعلومات لا يعد أمرا جديدا، بل يعد هاجسا تاريخيا، وتسرب المعلومات أو التمكن من فك تشفيرها، يمكن أن يشكل منعطفا تاريخيا ومنفعة كبيرة في العديد من الأحيان مثل ما قمنا بتوضيحه سابقا فيما يخص آلة إنيغما، من جانب آخر يمكننا أن نقول أن السايبرفوبيا هي أحد النتائج السلبية التي نتجت عن الرقمنة، فذا نظرنا إلى التاريخ يمكننا أن نرى التخوف الذي يعاني منه ناس في كل مرة يعتمدون فيها على شيء لا يفهمونه بطريقة جيدة، أو صحيحة، فالنموذج الحالي للتعامل مع التكنولوجيا، وفي العديد من الإجراءات، تطلب منا العديد من البيانات المالية والشخصية، والتي ما كنا لنوفرها لأي كان من قبل، هذا النموذج الجديد في العيش لم يتلاءم معه الجميع، فحتى لو اعتبرنا أن المرحلة التي نعيش فيها اليوم هي بمثابة مرحلة انتقالية فقط، إلا أن الإنسان، سيبقى دائما يخاف من كل شيء لا يفهمه، الأمر الذي دفع بالعديد من الأشخاص إلى رؤية هذه التكنولوجيا على أنها اقوى من أن يتم الاعتماد عليها فقط، خاصة في العمليات التي تتعدى القدرة الإنسانية على الاستيعاب، مثل ما وضحنا سابقا مع التبادل الفائق السرعة، أو استخدام الآليين، أو الخوارزميات من اجل تحديد الأهداف العسكرية وإلحاق الضرر، فالآلة لا أخلاق لها، والإنسان عليه دائما أن يكون المرجعية الأخيرة في اتخاذ القرار، وليس مجرد خوارزمية معينة، أو قرار آلي يستند إلى معطيات تتعلق بالاحتمالات.

فمما لا شك فيه، فإن هذا النوع من الفوبيا، ونحن نتكلم هنا عن السايبرفوبيا؛ يكون قد بدا مع تزايد استخدام الشبكة العالمية، أو مع تحررها وخرجها للعامة، ويبدو أن توسعها، وبداية دخولها للحياة الشخصية للإنسان هي التي ولدت هذا الشعور بداية التسعينات، ونجد أن **إدوارد لوكس** (Edward Lucas) يقول في هذا السياق: [149]

> **"ففي بداية تطوير الحواسيب والإلكترونيات، لم يكن التفكير مركزا بشكل أساسي على قضايا الخصوصية وتسرب المعلومات، بل كان التركيز أكثر على القدرة، والإنتاجية، إلى جانب قضايا عرض المعلومات".**

---

[149] Edward Lucas, ***CyberPhobia, Identity Trust Security and Internet*** (United Kingdom: London, Published by Bloomsbury Publishing, the First edition, 2015.), p. 22.

ولهذا يمكننا أن نرى أن قضايا الخصوصية، لم تكن أهم شيء يدرس أثناء التحول التكنلوجي الذي حدث، فحتى لو كانت هناك قضايا تتعلق بسرية المعلومات منذ القدم، إلا أن الصيغة القانونية التي تتعلق بالخصوصية وتنقل المعلومات بالطريقة التي نعرفها اليوم لم تكن موجودة من قبل رغم اهتمام العديد من الباحثين بهذا الأمر.

يمكننا النظر إلى هذه الفوبيا حاليا على أنها حالة جديدة من الصراع، وأصبحت تدرس على نطاق واسع، إذ أن المعلومات وخاصة بعد تطور خدمات الهواتف النقالة، وتقدم التكنولوجيا أيضا وتعقدها أكثر، جعل من الأمر أكثر صعوبة للجميع من اجل فهم أين تذهب معلوماته، وأين يتم تخزينها، وما هي المنافذ أو الأبواب الخلفية الضعيفة التي يمكن اعتمادها أو استغلالها لسرقة المعلومات،[150] فهذه الأفكار التي تعبر عن العجز الواضح للفرد أمام هذا العالم المتغير، كما تعبر أيضا عن العجز أمام الحكومات التي تريد استغلال هذا الأمر لصالحها عبر جميع البيانات، والحصول عليها، الأمر الذي يدفعنا إلى تفهم المجهودات الكبيرة التي يبذلها المجتمع الإلكتروني في توفير أفضل الطرق من اجل تعمية المعلومات، والحفاظ عليها، حتى أنه يمكننا أن نرى حاليا أن القضايا التي أصبحت تشكل هاجسا وتغذي هذه الفوبيا، هي القضايا التي تتعلق بالخصوصية، وبعض الشركات الكبرى فهمت جيدا الرسالة، واعتمدت على هذه النقطة لجلب عدد إضافي من المستخدمين.

يجب معرفة أن السايبرفوبيا تعد أحد أنواع رهاب التكنولوجيا (Technophobia) ، أي التخوف كما قلنا سابقا من أي اختراع، أو تطور تكنولوجي مهما كان، ولهذا فالأمر لا يتعلق فقط بالفترة الحالية إذ أخذنا بالتكنوفوبيا؛ فهذا التخوف يمكن أن يترجم عبر الخوف من الحواسيب في المنزل، أو العمل، وأي شيء له علاقة بالتقانة، ويمكننا أن نرى ذلك مثلا عند محاولة الدولي القيام بتحديث مؤسساتها العمومية عبر استخدام حواسيب، بدل الأوراق، إذ نجد في الغالب رفضا كبيرا من قبل العمال القدامى لهذه العملية للأسباب غير موجودة.[151] فالتكلم

---

[150] Joong Gyu Ha, Tom Page, Gisli Thorsteinsson, "**A Study on Technophobia and Mobile Device Design,**" in ***International Journal of Contents***, No 2, Volume 7(Jun, 2011), pp. 17-25.

[151] Martin Bauer, ***Resistance To New Technology, Nuclear Power, Information Technology and Biotechnology*** (United Kingdom: Cambridge, Published by The Press Syndicate of The University of Cambridge, first paper edition with corrections, 1997), p. 102.

علـى الفوبيـا التـي تتعلـق بالتقانـة يمكـن أن تكـون واسـع جـدا، كمـا يمكـن أن تكـون جـد متخصصـة مثل ما هو الحال مع الدراسات التي تتعلق بفوبيا الحواسيب.[152]

ولهذا، ووفق المعطيات التي عرضناها، يمكن تحديد المميزات، والخصائص التي تقوم عليها السايبرفوبيا وفقا لما يلي:[153]

1. مقاومة كبيرة في التكلم على أي شيء له علاقة بالحواسيب، والتقانة.
2. انزعاج كبيرة، وعام بالآثار الذي تركته التقانة، والحواسيب على الحياة الاجتماعية.
3. عدائية، وتشاؤم كبيرة في أي شيء له علاقة بمستقبل الحواسيب، والتقانة.
4. الرغبة في تدمير أي مصدر للتقانة، أو القدرة الحاسوبية.

في الأخير، يمكن القول أن التقانة كانت لها إفرازات كبيرة على العالم الذي نعيش فيه اليوم، فالحالة التي درسناها هنا، تبين بشكل واضح العمق الذي ذهبت إليه التقانة في الحياة الشخصية للناس، فعرض مثل هذه المعلومات يبين لنا فعلا الانعكاسات التي يمكن أن تؤكدي إلى استخدام مثل هذا التوسع التقني الذي أصبح يعتبره البعض على أنه امتداد طبيعي للتطور، في توطيد عمليات السيطرة العالمية، فمثل ما هو الحال مع النموذج الرأسمالي، أو العولمة، فالدول المسيطرة في العلاقات الدولية، دائما ما تسعى إلى تصدير، وإقامة نموذج، تكون متأكدة أنها الرابحة فيه، وفي هذه الحالة، هو نموذج عالم معولة، أين يصبح الجميع تحت الرقابة المستمرة، وتحت السيطرة التامة، كون كل مصادر عيشه، وكل تعاملاته، وكل مصالحه، أصبحت مربوطة إلكترونيا؛ فمثل ما تم التعبير عليه في العلوم الطبية فيما يخص أن بعض الأمراض التي لها علاقة بالحساسية (Allergy)، فالجسم يمكنه أن يطور هذا المرض كطريقة للدفاع عن نفسه من بعض المواد المصنعة، أو الكيميائية، لهذا يمكن من جانب آخر النظر إلى الرغبة في المقاومة لمن يعانون من السايبرفوبيا على أنها مؤشر للخطر أكثر منه مرض يجب التعامل معه،

---

(152) Stephen J. Hines, Steven A. Seidman, "The Effect of Selected Cai Design Strategies on Achievement, and an Exploration of Other Related Factors," edited by Michael R. Simonson and Jacqueline Frederick, **10th Annual Proceedings of Selected Reserch Paper Presentation at the 1988 Annual Convention of the Association for Educational Communication and Technology**, (The united States of America: Los Angeles, published by the educational Ressource Information Center, the first edition, 1988), pp. 372-383.

(153) Martin Bauer, ***op. cit***, pp. 103.

لماذا ؟ لأن الشكل الحالي للتقانة خارج عن السيطرة، ولا يمكن لأي كان التحكم بها، أو رقابتها بشكل تام، أو التكهن بها، الأمر الذي سيلعب في الاستخدامات الغير قانونية، والغير أخلاقية لهذه التقانة.

في نهاية الجزء الأول من دراستنا، يمكننا أن نرى أن دراسة الأمن الإلكتروني، وعلاقته بالهيمنة في العلاقات الدولية، هو امرأ يجب التعاطي معه بطريقة ممنهجة، وواسعة، ومتخصصة، ذلك أن طبيعة الموضوع تتطلب التعاطي مع إشكالية البحث من زوايا متعددة من اجل محاولة فهم وتحليل الموضوع القيد الدراسة؛ فالتطور التقني كان له تأثيرا كبيرا على مختلف المخرجات السياسية والاجتماعية في العصر الحالي، ويمكننا أن نرى ذلك، عبر تتبع مختلف القرارات السياسة، والاستراتيجيات التي تعتمدها الدول في العلاقات الدولية، لهدف الهيمنة، أو تحقيق مصالحها المختلفة. ففي ظل هذا العالم الذي اصبح يعتمد على التكنولوجيا بشكل مزايد، بدى من البديهي جدا أنه سيكون هناك إشكال كبير يتعلق بالأمن الذي له علاقة بهذه التقانة، فالتعاطي مع مسالة الأمن الإلكتروني، أصبحت تشير إلى ذلك المنهج الجديد التفاعلي، المتداخل، في معالجة البيانات والمعلومات، ففي ظل هذا العالم الأكثر تقاربا، والأكثر تشابكا، والأكثر اعتمادا على الآخر، بدا من الواضح جدا أن معالجة هذه الظاهرة الأمنية ستتطلب منا فهم مختلف الارتدادات التي أحدثتها التقانة، والتي يمكننا أن نرى أنها طالت معظم جوانب الحياة الإنسانية، فقد اصبحنا الآن نعيش في عالم أصبحت الرقمنة تجسد معظم أشكال التفاعلات الاجتماعية، والسياسية، والاقتصادية.

ويمكننا فهم ذلك من خلال المفاهيم التي قمت بعرضها، وحاولت التعمق فيها، وذلك من أجل محاولة إيضاح مختلف نقاط الوصل، ومختلف الأوعية التي تربط مختلف التخصصات ببعضها البعض، كما أن الهدف أيضا كان موجه لتكوين حوصلة فكرية، بمثابة تحيين للمعلومات لما وصل إليه العلم حاليا، فمن اجل فهم ما يمكن للتقانة أن تقدمه وتحدثه حاليا، وخاصة فيما يخص التطبيقات الأمنية، والعسكرية، على أي شخص أن يكون على دراية ببعض المفاهيم الأمنية التي لها علاقة بالأمن الإلكتروني وأساليب الهيمنة، كما يجب أن تكون هناك أيضا دراية بالاستراتيجيات الأمنية الجديدة، والتقدير الجديد لمصادر القوة والثروة في العلاقات الدولية.

فإذا الأمن الإلكتروني، وبعض الهياكل التي يقوم عليها، يمكننا أن نرى أنه رغم تنوعها، ورغم تعدد الإجراءات الأمنية التي تقوم عليها، إلا انه من الصعب جدا توفير الأمن المطلق والنهائي، فمعظم المفاهيم التي قمنا بعرضها في هذا الجزء من البحث، سواء تلك التي تتعلق بالانعكاسات الاجتماعية

للثورة التكنولوجية، أو الانعكاسات على قضايا التنظير، كما الانعكاسات على أساليب الدفاع والأمن والتقدير العسكري الاستراتيجي؛ يمكننا أن نجد أن الشيء الوعيد الذي أصبح يميز الأمن حاليا، أو الأمن الذي يعتمد على قاعدة على إلكترونية من أجل تشغيله، وتفعل البروتوكولات التي يقوم عليها، هو أن الأمن الإلكتروني التام، لا يمكن تحقيقه، الأمر الذي سيجعل مع قضايا الهيمنة، ومحاربة الهيمنة، أحد الأساليب الجديدة للصراع الدولي، ويمكننا أن نفهم هذه الفكرة جيدا، في الطرح الذي قام به **بروس شنايدر** حيث يقول: (154)

> "**بكل بساطة، يجب علينا أن نحرص على الأقل، على أن الأشخاص الذين يقومون بمثل هذه العمليات، هم يضعون أنفسهم في خطر، أو يكونوا معرضين للخطر**".

أي أن يكون الخطر واحتمال الضرر الذي يمكن أن يتعرض له الشخص الذي سيقوم بعملية غير قانونية في الفضاء الإلكتروني في عرضة مستمرة للخطر، فحاليا اصبح من الصعب جد الأخذ بالأمن التام، ولهذا اصبح يتعامل مع الأمر بمنطق إدارة المخاطر، وهامش الخطر المقبول، فمعظم المفاهيم التي قمنا بمعالجتها، تشير إلى الانفلات الكبير في التحكم، والسيطرة، واحتكار القوة، فالعالم في تغير واضح، ويبدو أنه سيصبح رقمي أكثر من ما هو علي حاليا، فمعظم المفاهيم التي تطرقنا إليها تشكل إلى جزءا صغيرا من ما هو عليه العالم الرقمي فعليا، العالم الذي سيحدث تغييرا، في طريقة تفكيرنا، وطريقة معالجتنا للمشاكل، وأساليبنا في الصراع، والعيش بصفة عامة.

(154) Bruce, Schneider, ***op. cit***, p. 222.

2.0 إطار نظري

لقد شكل الأمن أحد أهم المتغيرات التي اهتم بها المنظرين في العلاقات الدولية، وذلك عبر دراسة، طريقة تحصيل الأمن، والأساليب التي تعتمدها الدولة من أجل تحقيق الأمن، كما العديد من القضايا التي لها علاقة بالسيادة، وتطور الفواعل في العلاقات الدولية، والركائز التي يقوم عليها الأمن وتطوره، وتغير النظرة العالمية للأمن، مثل ما هو الحال مع بروز الأمن الإنساني. لكن يجب أن نعرف أيضا أن الأمن يعد من أهم المتغيرات في العلوم العسكرية، والاستراتيجيات العسكرية، وأساليب الإكراه والسيطرة العالمية، كما أن الذي يهمنا هنا، هو الاعتبارات المادية، أو اللوجستية التي كان يعبر عليها مفهوم الأمن، وذلك عبر رؤية مختلف الأنماط التي كانت تستند عليها الهيمنة، والقوة في العلاقات الدولية، ففي الحرب العالمية الأولى والثانية، يمكننا أن نرى أن السيطرة والقوة والهيمنة على الآخر، كانت لها علاقة أكثر، بالعتاد العسكرية، والأسلحة التقليدية، والشبه تقليدية مثل ما هو الحال مع الأسلحة الكيماوية التي تم استعمالها، بالإضافة إلى السيطرة البحرية، والجوية، بل يمكننا حتى التطرق إلى العقيدة العسكرية التي كانت تعبر على شروط القوة أثناء الحرب، مثل ما هو الحال مع عنصر الإنتاجية، والذي يعبر على قدرة دولة ما على تعويض عتادها الذي دمر في ساحة الحرب بشكل أسرع، بالإضافة إلى طريقة تفكير تقليدية قائمة على السيطرة المكانية على مناطق محددة.

يمكن اعتبار تخلي منظمة حلف الشمال الأطلسي(NATO) على خط ماجينو(Maginot Line) سنة 1960 الموجود في فرنسا، على أنه تغير فعلي في العقيدة العسكرية، ومفهوم الأمن، والقوة أيضا، إذ أن استراتيجيات التي كانت تقوم على الدفاعات الخطية، وأساليب الهجوم الخطية والتي تعد حرب الخنادق أحد أشكالها (Trench warfare)، لم تعد مفيدة في ظل المعادلة الجديدة القائمة على قدرة الردع النووية؛ ومن هنا يمكن القول أن نفس الأمر حصل مع الانفجار الإلكتروني، وتوسع الشبكة العنكبوتية العالمية، وإدراج الأنظمة الإلكترونية، وأنظمة التحكم، حتى في استخدام الأسلحة النووية، والعتاد الحربي الحديث، فالحرب الإلكترونية، والهيمنة الإلكترونية، والمقاومة الإلكترونية، تمثل صراعا يحدث بسرعة الضوء، صراع على سلم عالمي، والجميع معني به، وكل شخص، يمكنه أن يشارك في هذا الصراع، ويمكنه أن يختار أي طرف يريد. بروز الأمن الإلكتروني، أو الحرب الإلكترونية أدرى إلى بروز العديد من ردود الأفعال، كما أدى أيضا إلى بروز العديد من المحاولات النظرية التي تدرس موضوع القوة، والهيمنة، والعلاقات الدولية، وذلك من اجل محاولة فهم الوجه الجديد لهذا العالم الرقمي الذي أصبح يتضمن مختلف أنماط، وأشكال، وتفاعلات الإنسان، الأمر الذي سيؤثر بطبيعة الحال على طريقة عيش

الإنسان، وطريقة رؤيته للآخر، وطريقة محاربته للآخر، وطريقة مكافحة لأي شيء يتعارض ومصالحه الأساسية، أو تلك التي لها علاقة بأيدولوجيات معينة.

2.1 الأمن الإلكتروني في الدراسات الأمنية

لقد تطرقت في عرضي للمفاهيم، وخاصة في الشق الذي تعلق بالأمن والأمن الإلكتروني، على بعض التحولات التي طرأت على مفهوم الأمن، وطريقة تفاعل العديد من المنظرين مثل ما هو الحال مع **جوزيف ناي** الذي حاول أن يناقش بروز الأمن الإلكتروني، أو متغيرات القوة التي لها علاقة بالبوابة الإلكترونية، فالأمن الإلكتروني يطرح تحديا جديد في مجال الدراسات الأمنية كونه يعبر من جديد وكما حصل في نهاية الحرب الباردة، على لامركزية أوسع للأمن وتعدد كبير في مختلف الأدوات، والمحددات الأمنية في الوقت الحالي، فقد أصبحت الدراسات الأمنية حاليا في حقل جديد عليها التعامل معه، فكما كانت أسلحة الدمار الشامل عنصرا أساسيا في المعادلة الدولية والتنظير ، كذلك هو الأمن الإلكتروني، أو الأسلحة الإلكترونية، فرغم أنه الموضوع يعد جديدا، إلا أنه يمكننا أن نرى العديد من المحاولات، من أجل قولبة هذه الظاهرة الجديدة، ومعرفة الوزن الحقيقي الذي لهذه الظاهرة حاليا ومستقبلا كما صرح ناي فيما يخص المزارع والحب.

قبل التعمق في الموضوع أكثر، وكما سنرى فيما بعد مع السبرانية، فإن النقاش الذي يربط عالم التكنولوجيا، بعالم السياسة، بعالم التنظير، يعد حقيقة لا يمكن إنكارها، خاصة كوننا نهتم أكثر هنا، بتأثير التقانة على حقل التنظير والسلوك الاجتماعي والصراع من اجل الهيمنة؛ ويمكننا أن نرى ذلك مثلا في ما اصبح يطلق عليه الآن : مجموعة العشرة (Le Groupe des dix)، هذه المجموعة لا علاقة لها بدول، أو مجموعات اقتصادية محددة فقط، بل تعبر على مجموعة من التجمعات التي حصلت في فرنسا بين 1969 و1976، هذه التجمعات تمثل مجموعة من الفلاسفة، والاقتصاديين، والأطباء، وعلماء الاجتماع، والبيئيين، والسبرانيين، والسياسيين، والمنظرين ... من مختلف أنحاء العالم، وذلك لوجود قناعة أن هذه التفاعلات التي تحدث يجب النظر إليها بصورة أكبر، ومن جانب آخر فتجمع العشرة، كان يهدف أيضا إلى دفع النقاش إلى عمق أكبر من اجل كسر الحواجز بين التخصصات، فالرغبة الأساسية كانت محاولة

تقريب ما هو سياسي إلى ما هو علمي، من اجل فهم أفضل للتفاعلات التي تحدث في الواقع، [155] والتي يمكننا أن نراها في طريقة تعامل السياسيين أو المنظرين مع الواقع المعاش، ومع المستجدات التي تطرح أو تفرض نفسها.

هناك أيضا من يرى أن التقانة، وخاصة مع بروز الشبكة العالمية ساهم في بروز طرح القوة الناعمة بشكل اكبر، [156] إذ أن القاعدة الإلكترونية التي تعتمد عليها الصراعات الإلكترونية، لا تعد مدمرة، ولكنها تميل أكثر إلى تحقيق مصالح قائمة على المعلومات، ولما نتكلم على المعلومات هنا، فنحن نتكلم على مصادر الثروة التي لها علاقة مباشرة بالرقمنة، أي كل شيء تقريبا. من الواضح جدا أن الاهتمام النظري بالأمن الإلكتروني والإفرازات التي جاء بها أصبح شيء ضروريا يجب التعاطي معه، ولكت رغم هنا، يمكننا أن نرى وجود نقص كبير في التطرق إلى الأمن الإلكتروني، بنفس الاهتمام الذي ناله الأمن الإنساني أو الأشكال التقليدية للأمن مثلا. من هنا يمكننا أن نقول أن التعاطي مع الأمن الإلكتروني من منطلق النظريات السائدة، سيتبع نفس العقيدة، أو الذهنيات التي جعلت من الجميع يناقش قضايا الأمن الإنساني.

2.1.0 الواقعية

يتكلم جيمس أدامس (James Adams) والذي ينتمي إلى تيار الواقعية الجديدة على الأمن الإلكتروني وإفرازاته على العلاقات الدولية، ويصرح أن:[157]

"**الفضاء الإلكتروني، أصبح ميدانا جديدا للصراع الدولي**".

فجيمس يرى مثلا أن الأمن الإلكتروني وخاصة الأنترنت، تمثل التصور الواقعي بامتياز، إذا لا توجد هناك قوة سياسية، أو جهة معينة يمكنها التحكم في الشبكة، في إشارة واضحة إلى الطرح الواقع الذي يتكلم على عدم وجود سلطة في المجتمع الدولي، أو حتى طرح بعض المفكرين أمثال **جون ميرشايمر**

---

[155] Véronique Anger, ***Sure Les Trace du Groupe des dix*** (France: publier par le Forum Changer d'Ère - Forumchangerdere.com, 2013), p. 6.

[156] David Bollier, ***The rise of Netpolitik: How The Internet Is Changing Politics and Diplomacy*** (The Unites States of America: Washington D.C, published by The Aspen Institute, 2003), pp. 17-26.

[157] James Adams, "Virtual Defense," in: ***https://goo.gl/tBbUvf***, (Thursday, May 26, 2016).

(John Mearsheimer) و**كينث والتز** (Kenneth Waltz 1924-2013) حول موضوع هيكلية النظام الدولي (الواقعية البنيوية) وقضايا الواقعية الدفاعية والهجومية،[158] فكل دولة في هذا العالم الإلكتروني تقف وحدها مع حلفائها المحتملين، وسيكون من الصعب جدا أن تثق دولة في دولة أخرا، فكل دولة ستكون مجبرة على بناء قوتها الإلكترونية، مع الإبقاء على الحذر المستمر من أي دولة أخرى يمكنها أن تخترق الدفاعات الذاتية؛ ويمكننا فهم هذه الفكرة في تعبير المدير السابق للاستخبارات الأمريكية، ووزير الدفاع الحالي **ليون بانيتا إدوارد** (Leon Panetta) حين قال:[159]

"**يجب علينا أن نحرص على أن لا يحصل لنا سايبر– بيرل هاربر**".

يمكننا أن نرى هنا إشارة واحدة إلى هجوم بيرل هاربر (Pearl Harbor) الذي حصل في 7 ديسمبر 1941، ومما لا شك فيه، الإشارة هنا لها علاقة أكبر بالخسارة الكبيرة الناتجة عن عدم الاستعداد للهجوم، والفكرة التي يطرحها **بانيتا**، تعكس التفكير الواقعي بامتياز، أي الاستعداد واكتساب القوة اللازمة في ظل عالم مجهول المعالم، بل يمكننا حتى أن نقول أن الأنترنت كما قال **أدامس**، تعزز أكثر فكرة المجهول ومعرفة نوايا العدو، الأمر الذي سيعزز عدم الشعور بالأمان، فمن جانب آخر يمكننا أن نرى أن الاهتمام هنا كان أكثر بالجانب العسكري التي له علاقة مباشرة بالحرب والسيطرة على ميدان الحرب السائد.

لقد عرفنا من قبل أن الواقعية دائما كانت تركز أكثر على دور الدولية المهم في العلاقات الدولية، إلى جانب بحثها المستمر على تحقيق مصالحها، وأن القوة، والأمن يمثلان قلب هذا التوجه النظري الذي يناقش فكرة عدم وجود سلطة عليا في النظام الدولي. لقد حاول **كينث والتز** تحويل الاتجاه الواقعي إلى نظام علمي دقيق، أما ميرشايمر في المقابل، وخاصة في كتابه المآسي السياسية للقوى العظمى (The Tragedy of Great Power Politics) نجد أنه يحاول ملأ الفراغ الذي تركه والتز في القضايا التي تتعلق بالمنهجية المتبعة في دراسة السياسة الخارجية والأمن من منظور الواقعية الجديدة، فمبدئيا ينظر إلى الواقعية أنها لا تحتاج إلى إعادة النظر في مبادئها من أجل محاولة فهم الأمن في العصر

---

(158) John Mearsheimer, "Structural Realism" ***in International Relation Theories, Discipline and Diversity***, Edited by Tim Dunne, Milja Kurki, Steve Smith (United Kingdom: published by Oxford University Press, the 3rd edition, 2013), pp. 2-16 .

(159) Elisabeth Bumiller, Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack," in**:** ***http://goo.gl/WCm5Gv*****,** (Thursday, May 26, 2016).

الإلكتروني، فالأمن الإلكتروني من منظور الواقعية، يمكن التأقلم معه من نفس منطلق عمليات التأقلم التي مرت على الواقعية من قبل مع مواضع الاعتماد المتبادل، والفواعل الغير رسمية، والعولمة. [160]

فالواقعية يمكنها أن تتعاطى مع القضايا التي لها علاقة مباشرة بالقاعدة الإلكترونية مثل ما هو الحال مع الاقتصاد، والذي يمكن أن يشكل تهديدا مباشرات لأمن الدولة، ولكنها لا تتعاطى مباشرة مع القضايا الإلكتروني كتهديد، خاصة أنه هناك العديد من الواقعيين الجدد الذين يدرجون الأمن الإلكتروني في الإطار العسكري للصراع وليس كحقيقة وظاهرة متكاملة يجب التعاطي معها على حدة. [161]

ولكن رغم هذا، هناك من الواقعيين من يرى أن الحرب الإلكترونية، وما يمثله الأمن الإلكتروني، يعد شيء ملح وسيفرض نفسه، كونه يعبر عنصر جديد في طريقة تسيير الصراعات، ويعد تحول على التفكير التقليدي الذي أن سائدا، [162] فإذا كانت الحرب النفسية أحد أهم متغيرات الحرب كما صرح **صن تزو**، فميدان الحرب الإلكترونية يمثل أحد تلك المتغيرات، ولما نتكلم على الحرب الإلكترونية، فنحن نتكلم أيضا على مختلفة الحروب التي تدخل تحت مضلة هذه الحرب كما وضحت ذلك سابقا في إطار المفاهيم.

2.1.1 الليبرالية

تعبر الليبرالية على ذلك الاتجاه في العلاقات الدولي الذي يعطي أهمية أكبر موضوع تعدد الفواعل فالعلاقات الدولة، بالإضافة إلى الدور المهم للمؤثرات الداخلية على المخرجات السياسة الخارجية للدولة، كما أيضا الدور المهم للمؤسسات الدولية والفواعل الرسمية والغير رسمية، وذلك في ظل دفع الدراسات الأمنية إلى أبعد من التعاطي البسيط الذي يستند إلى أفكار هوبس (Hobbesian) التي تتعاطى مع كيفية تحقيق البقاء في ظل هيكلية للنظام السلطوي في العالم.

---

(160) Johan Eriksson, Giampiero Giacomello, "The Information Revolution, Security, and International Relation," in **International Political Science Review**, No 3, Volume 27 (2006), pp. 212-224.
(161) Loc. cit.
(162) Lonsdale DJ, "Information Power: Strategy, Geopolitics, and the Fifth Dimension," in ***Journal of Strategic Studies***, No 2-3, Volume 22 (1999), pp.137-57.

بشكل عام يمكننا القول أن التقدم التكنولوجي، والتقني يصب في صالح الطرح الذي تهدف إلى الليبرالية، خاصة ذلك الطرح الذي يتعلق بكيفية توفير السلام العالمي، والدور الذي يمكن أن يلعبه الاعتماد المتبادل في ذلك، الأمر الذي يمكن أن يؤدي إلى تعاون امني، وإقامة مجموعات امنيه من اجل تحقيق السلم، أو المحافظة عليه.[163]

إن مسال الأمن الإلكتروني، وتأثير العصر الرقمي على مفهوم الأمن لم يتم تجاهله بطريقة كاملة في النظرية الليبرالية، إذا هناك بعض من المنظرين في التيار الليبرالي الذي أدركوا التحدي الجديد المتمثل في ثورة المعلومات، خاصة لما ننطر إلى طرح كل من **جوزيف ناي** و**روبرت كيوهان** (Robert Keohane) في النماذج والطروحات التي قدماها في يخص الاتصالات المعقدة، والاعتماد المتبادل العميق بين الدول؛ ذلك أن الأمن الإلكتروني والتحديات الأمنية الجديدة التي سببها، ينظر إليها خاصة من الجانب الاقتصادي، أي تأثير ثورة المعلومات هذه على القضايا التي تتعلق بالاعتماد المتبادل.[164]

يرى ناي أمن الدولة على أنه يعبر على غياب التهديد ضد مختلف الركائز الحيوية التي تقوم عليها الدولة، ولكن رغم هذا، لم يتعامل ناي مع الأمن الإلكتروني كمنطلق منهجي لمعالجة القضايا التي تتعلق بالأمن رغم أنه لا يرف ذلك ويقر بوجود هذا النوع الجديد من الأمن كما وضحت ذلك في إطار المفاهيم، فناي يقول أن القوة الناعمة حضت بأهمية كبيرة جدا لم تحضي بها قبل بسبب الثورة الرقمية، وأن الأمر يعود إلى توفر العديد من قنوات الاتصال التي تخترق سيادة الدولة بكل بساطة،[165] لكننا نعرف هنا أن القوة الناعمة تجسد مجموعة من الأفكار والمفاهيم، ولا تتطرق إلى الوسائل المادية في أجل القيام بذلك.[166]

---

[163] Johan Eriksson, Giampiero Giacomello, "The Information Revolution, Security, and International Relation," ***op, cit.***

[164] Joseph Samuel Nye, **Understanding International Conflicts: An Introduction to Theory and History** (The united States of America: New York, published by Pearson and Addison Wesley, 4th edition, 2003), pp. 199-202

[165] Joseph Samuel Nye, **Power in the Global Information Age: From Realism to Globalization** (United Kingdom: London, published by Routledge, the first edition, 2004), 81-96.

[166] Johan Eriksson, Giampiero Giacomello, "The Information Revolution, Security, and International Relation," ***op, cit.***

يمكننا أن نرى أن الليبرالية، وفي معالجتها للأمن الإلكتروني، وتأثير ثورة المعلومات على الدراسات الأمنية في هذا الخصوص، تركز أكثر على التطرق إلى الآثار التي أتى بها هذا الأثر، ولا تتطرق بشكل مباشر إلى الأمن الإلكتروني، فهي مثلا تعالج القضايا التي لها علاقة بالفواعل الغير رسمية في العلاقات الدولية وكيفية تأثير الأمن الإلكتروني على مثل هذه القضايا، خاصة في النقطة التي تتعلق بالاندماج الكبير الذي حصل بين مختلف القطاعات العسكرية والاقتصادية والاجتماعية، وتشابك العلاقات بطريقة أعمق في العلاقات الدولية. في الأخير فإن السؤال الذي يطرح حول قدرة نظرية أقيمت بشكل أساسي في الأول لتعالج القضايا الاقتصادية والسياسية من استيعاب إفرازات الثورة المعلوماتية يبقى مطروحا. [167]

إن التهديد الأمني الإلكتروني والتحديات التي لها علاقة بثورة المعلومات، تعد واضحة، وهي تدفع العولمة إلى مسافة ابعد من التي كانت عليها، الأمر الذي سيؤدي في المقابل إلى إضعاف سيادة الدولة، والليبرالية كباقي النظريات تحاول التأقلم مع هذه الظاهرة الجديدة، ولكن يمكننا أن نرى أن التعامل مع مثل هذه القضايا يعد جد صعب، ومعظم الذي طرحناها هنا يشير فقط إلى نوع من الإسقاط النظري والعملياتي للتحديات الأمنية التي فرضتها ثورة المعلومات

2.1.2 البنائية

لقد كان للنظرية البنائية تواجد أكبر في العلوم الأنثروبولوجية ودراسات علم الاجتماع، قبل أن تجد لها طريقا إلى العلاقات الدولية، حيث أصبحت بداية التسعينات من بين أبرز النظريات في العلاقات الدولية خاصة بعد الأزمة التي كانت منها كل من النظرية الليبرالية، والواقعية مع نهاية الحرب الباردة. فمن ناحية الطرح الأنطولوجي والأبستمولوجي، يصرح منظري النظرية البنائية أنهم أصبحوا يمثلون الجسر وأرض الوسط (Middle Ground) بين الطروحات التقليدية والجديدة في العلاقات الدولية (ما بعد الحداثة). [168]

ولهذا يمكننا أن نفهم من هنا أن المتغيرات الاجتماعية سيكون لها بروز اكبر في تحليل الأوضاع السياسية والدولية في النظرية البنائية، بالإضافة إلى هذا، وفيما يخص الأمن، يمكننا أن نرى أن البنائية، ومن اجل المعالجة المنهجية لهذا الموضوع، تم البحث في نظرية الأمننة؛ يمكننا أن نقول هنا أنه رغم

---

[167] Loc. cit.

[168] Colin Wight, "Philosophy of Social Science and International Relations," in ***Handbook of International Relations***, edited by Walter Carlsnaes, Thomas Risse, Beth A. Simmons (United Kingdom: London, published by SAGE Publication, the first edition, 2002), pp. 23-45.

تأثير الدراسات النقدية على مفهوم الأمن، وعلى التصور الذي كان سائد فيما يخص التهديد العسكري، أو الاقتصادي، أو الأوسع مع الأمن الإنساني،[169] إلا أن الأمن الإلكتروني أعاد طرح كل هذه الأسئلة من جديد حتى وإن كانت النظرة تختلف عند البعض في طريقة التعامل مع هذا التهديد والمفهوم الجديد، فقد عبرت **لين هانسن** في تكلمها على بروز هذا النوع الجديد من التقانة والتحول الأمني، والأمن الإلكتروني، على أنه بمثابة الكارثة الرقمية (Digital Disaster)، فقد طرحت **لين** العديد من الأفكار التي لها علاقة بمدرسة كوبنهاغن (Copenhagen School)، خاصة وأن المنهجية التي عالجت بها المدرسة الأمن الإلكتروني جعلت من الظاهرة غير ديناميكية، وذلك عبر التصريح مثلا بأن الأمن الحاسوبي لا يمكن اعتباره كأحد قضايا الأمن، وأن أي قضية تتكلم على تحول الأمن إلى أمن إلكتروني، يجب أن يجسد وفق الطرح التي يعالجه النقاش حول الأمننة (Securitization).[170]

ولهذا نجد أن التعاطي مع موضوع الأمن الإلكتروني يركز على البحث في كيفية إدراج النظام المعقد الذي تمثله هذه الظاهرة الجديدة في النقاش الدائر حول الأمننة بطريقة تسمح بإبقاء ما يعبر عنه الأمن الإلكتروني، والذي يعبر في راي **لين** على أمن الدولة، والأمن الوطني، الأمن الخاص، وأمن الشبكات؛ لهذا تم الإشارة إلى ما يسمى بالأمننة السبرانية أو الإلكترونية (Cyber securitizations)، بالإضافة إلى هذا ومثل ما هو مع قضية التداخل العلمي التي سنراها فيما بعد، نجد أن **لين** و**هيلين** أيضا يتكلمان على ضرورة نقاش بين تخصصي (Inter-disciplinary Discussions) من أجل محاولة الضبط المنهجي لهذه المعضلة الأمنية الجديدة.[171]

كما أن البنائية ناقشت أيضا القضايا التي تتعلق بتأثير الأمن الإلكترونية على الحرب، بالإضافة إلى المسائل المتعلقة بالهوية، ولهذا يمكن النظر إلى الحرب الإلكترونية على أنها صراع هوياتي أين كل الحدود التي كانت موضوعة سابقا تم تحديها والاعتداء عليها، وذلك في ظل الاختراق المستمر للسيادة، وبروز هوية جديدة، وهي الهوية الإلكترونية،[172] فالبنائية تعالج الأمن الذي له علاقة بالعالم الافتراضي عبر الأخذ بطبيعة الإمكانيات المستخدمة لتحقيق هذا الأمن، أو ممارسة الإكراه عن طريق هذه

---

[169] عامر مصباح، ***نظرية العلاقات الدولية*** (مصر: القاهرة، نشر من قبل دار الكتاب الحديث، 2009)، ص. 25.

[170] Lene Hansen, Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen Schoo," in ***International Studies Quarterly***, Volume 53(2009), pp. 1175-1155.

[171] Loc. cit.

[172] Saco Diana, "Colonizing Cyberspace: National Security and the Internet," in ***Cultures of Insecurity: States, Communities, and the Production of Danger*** , edited by Jutta Weldes, Mark Laffey, Hugh Gusterson, Raymond Duvall (The United States of America, Minnesota, published by the University of Minnesota Press, the first edition, 1999), pp. 261-292.

الإمكانيات، ذلك أن هذا الشكل الجديد من الأمن كما قلت سابقا، لا يتميز بنفس الدموية التي كانت تعبر عنها المفاهيم التقليدية، أو السائدة، فالبنائية اهتمت أيضا بالتأثير الرمزي لهذه الثورة الجديدة على بقية أشكال الرموز السياسية والاجتماعية مثل ما هو الحال مع الرمزية السياسية (Political symbolism) فالبنائية تحاول البحث على ما يوجد تحت الأرض وذلك بالتركيز على انعكاسات عصر الرقمنة على مختلف المقومات النظرية، إذ أن كونها تموضعها في الوسط كما قال أصحابها سيدفع بها إلى التعاطي مع مثل هذه القضايا بطريقة أكثر نقدية، وحذر.[173]

رغم أن كل الطروحات النظرية التي عالجتها في الأمن الإلكتروني في الدراسات الأمنية تتشارك في اعتبار الأمن الإلكتروني يعبر على قضايا جديدة، وأن الثورة المعلوماتية لها إفرازات يجب التعامل معها، إلا أنه يمكننا أن نرى أن التعاطي مع مثل هذه القضايا كان بمنهجية ترمي إلى التأقلم أكثر منها استكشافية، وربما يمكننا فهم ذلك كون الأمن الإلكتروني يعد ظاهرة جديدة، فعدم إيجاده بطريقة كثيفة في الدراسات النظرية التي تتطرق إلى العلاقات الدولية يشير كما راينا هنا، الصعوبة الكبيرة في التعاطي مع شيء يمكننا أن نرى بصمته في مختلف مستويات الحياة الإنسانية، فبداية بالواقعية إلى البنائية، يمكننا أن نجد أن كل نظرية، وجدت هذه الأثار أو البصمة، فإذ نظرنا إلى الأمر بصورة اكبر، سنرى أن الأمر يتعدى مختلف هذه الطروحات، ويدفع إلى تقريب وجهات النظر واستخدام منهجية أكثر استيعابا لهذه الظاهرة الجديدة، كذلك يجب أن أقول هنا أن هذه النظريات لا تعد الوحيدة التي تعاطت مع قضايا الأمن الإلكتروني، أو التي أشارت إليها. ولكن سيكون من الصعب جدا إيجاد مادة معرفة متعمقة في هذا النقاش، فالأمن الإلكتروني كمتغير ذو وزن في القضايا الأمنية الدولية بدأ يتبلور خاصة بعد 2000 بسبب أن معدل الخسارة أو الخطر بدا يطغى على معدل الأمان والسلم، وسيكمل هذه المسيرة إلى أن يصبح أحد المكونات الأساسية في التنظير في العلاقات الدولية،[174] لماذا ؟؛ لأن العالم سيصبح مرقمنا، ومعلوما إلى درجة سيصعب على

---

(173) Johan Eriksson, Giampiero Giacomello, "The Information Revolution, Security, and International Relation," ***op, cit.***

(174) Johan Eriksson, Giampiero Giacomello, **International Relations and Security in the Digital Age** (The united States of America: New York, published by Taylor and Francis E-Library, the first edition, 2007), p. 3.

أي أحد أن يفهم ماذا يحصل، بدون الإطلاع على ما يمثله الأمن الإلكتروني، والثورة المعلوماتية في الوقت الراهن، أو المعاصر لأي شخص يريد البحث في ذلك.

2.2 الأمن الإلكتروني والقانون الدولي

إذ نظرنا إلى مختلف أشكال القوانين الدولية والتي تم اعتمادها، والتي لها علاقة بالنزاعات، والصراعات الدولية، يمكننا أن نجد قصور كبير في التعامل مع القضايا التي لها علاقة بالأمن الإلكتروني، والأسلحة الإلكترونية، فرغم أن العديد من الدول لديها قوانين تضبط النشاط الإلكتروني، كما هو الحال مع القوانين التي تكافح الجريمة الإلكترونية، والقرصنة، والتجسس، وسرقة البيانات، إلا أنه على مستوى العلاقات الدولية، وخاصة مع الأهمية المتصاعدة التي أخذها الأمن الإلكتروني، بدا من الجد واضح أن التعامل مع ما يسمى بالأسلحة الإلكترونية، والحروب الإلكترونية، أصبح ضروريا، خاصة في ظل العديد من الأحداث التي برهنت على أن الصراع الإلكتروني العالمي، له القدرة على إحداث أضرار تفوق أضرار الأسلحة التقليدية بأشواط عديدة، وبطريقة سرية ولا يمكن تتبعها.

فإذا تكلمنا على القانون الدولي، وقضايا الصراع، ستتبادر في أذهاننا مجموعة من الأفكار التي لها علاقة، مثل ما هو الحال مع القانون الدولي الإنساني(International humanitarian law)، والذي يمكننا أن نجد في ضمنه مجموعة من الاتفاقيات المهمة التي حاولت حماية الحياة الإنسانية، والطبيعية أثناء النزاعات والحروب، كما حاولت أيضا أن تضبط كيفية إعلان الحروب، والحقوق المتعلقة بالدفاع على الإقليم، فقد عبرت اتفاقيات جينيف (Geneva Conventions)،[175] إلى جانب العديد من البروتكولات التي أتت بعد 1949 التي تطرقت إلى طريقة التعامل مع الضحايا، والأسرى، كما المساعدات الإنسانية، والسياسات التي تتعلق بالسلم والهدنة، والمنظمات الإنسانية الدولية المعترف بها؛[176] بل يمكننا حتى أن نجد أن القانون الدولي يتعامل أيضا مع القانون الجنائي الدولي (International criminal law) الذي يهتم بقضايا الأسرى والتجاوزات التي تحصل أثناء العمليات القتالية، بالإضافة إلى هذا لدينا ما يسمى بقانون الحرب(Law of war)، والذي يعد هو أيضا جزء من

---

[175] International Committee of the Red Cross, **What is International Humanitarian Law?** , Advisory Service on International Law, July, 2007.

[176] International Committee of the red Cross, **Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)**, Introduction to the Commentary on the Additional Protocols I and II, 8 June, 1977.

القانون الدولي العام، ويتعامل هذا القانون من القضايا التي تتعلق بإعلان الحرب، إلى جانب أجزاء من القضايا التي ذكرناها سابقا ذات الأبعاد العملياتية والإنسانية.

والحقيقة هنا أنه يمكننا أن نرى نمذجة للثقافة التي أرادت اتفاقيات جينيف إيصالها، كون الجميع معني لما يتعلق الأمر بالحرب، والأمر لا يتعلق فقط بالدولة، والجيش، فكون الحرب سلوك اجتماعي متوارث، يمكننا أن نجد عدة أمثلة جسدت الثقافة المتوارثة للسلوك الذي يجب إتباعه أثناء الحروب، فمن بين أبرز تلك الأمثلة، هي استعمال العلم الأبيض من أجل الاستسلام، فالعلم الأبيض علامة دولية للاستسلام، والأهم هنا هو معرفة أن استعمال العلم الأبيض للاستسلام يمكن تعقبه في التاريخ حتى إلى أسرة هان الثانية (Han dynasty) في الإمبراطورية الصينية سنة 25–225 قبل الميلاد،[177] واستمر استخدام العلم الأبيض إلى حد الآن، وأصبحت لديه قوانين تضبط طريقة استعماله أثناء النزاعات، كما أن استخدام العلم الأبيض لأغراض غير الاستسلام، يعد بمثابة جريمة حرب، وغدر في القانون الدولي، فالمادة 85 من برتوكول سنة 1977 الذي ادخل وأضاف بعض التعديلات على اتفاقيات جينيف فيما يخص ضحايا النزاعات الدولية، والذي تمت المصادقة عليه سنة 2013 من قبل 174 دولية ينص على:[178]

"أي استعمال لشعارات الحماية المعترف في اتفاقيات جينيف، من أجل خداع العدو، يعد بمثابة جريمة حرب".

من المهم هنا أن نعرف أن القوانين الدولية، دائما ما تحاول أن تعطي نماذج للسلوك الإنساني، وذلك استنادا إلى متغيرات أمنية، المادية منها والمعنوية، ولكن إذ نظرنا إلى الأمن الإلكتروني ووسائل الصراع الجديدة، يبدو لنا أنه من الواضح جدا أن التعامل مع هذه القضية سيحتاج تعمقا اكبر في الموضوع، فأشكال الصراع إلى حد الآن، وخاصة تلك التي تتميز بعمليات قتالة في الأرض والهواء والبحر، يتعامل معها بما يسمى قوانين أو قواعد الاشتباك (Rules of engagement) التي تعتمدها الدول من اجل تقنين القتال، وتوافق العمليات القتالية مع القوانين الدولية،[179] كما تعد أيضا جزء من تدريب الجنود الأكاديمي الذي يجب أن يعرفه أي جندي ذاهب للقتال في الأرض، والجهة المسؤولة على

---

(177) Brendan Koerner, "Why Do Surrendering Soldiers Wave White Flags?," in: ***http://goo.gl/bFxFDa***, (Friday, May 20, 2016).

(178) Suisse, Geneva, Academy of International Humanitarian Law and Human Rights, **Rules of Engagement**, October, 2011, p. 80.

(179) Alan Cole, Philip Drew, Rob McLaughlin, **Handbook on Rules of Engagements** (Italy: Sanremo, published by The International Institute of Humanitarian Law, 2009), pp. 1-4.

ذلك الجندي لديها مسؤولية قانونية فيما يخص ذلك،[180] أما عند التكلم على الأمن الإلكتروني، كأداة، أو كسلاح، يمكننا أن نرى قصور فعلي للقانون الدولي في التعامل مع الأمر، كما التعامل مع الأضرار التي يمكن أن تحدثها هذه الأسلحة، ولكن رغم هذا يمكننا أن نرى بعض المبادرات التي حاولت أن تعالج هذه القضية.

تعد اتفاقية بودابست للجرائم الإلكترونية (Budapest Convention on Cybercrime) التي تم الإمضاء عليها يوم 23 نوفمبر 2001 من قبل 50 دولة، أولى المعاهدات الدولية التي حاولت ضبط الجرائم الإلكترونية بطريقة قانونية، إذ أنها تعالج قضايا الملكية الفكرية، والإرهاب الإلكتروني، والقرصنة، ومختلف الجرائم الإلكترونية، أو الجرائم التي يتم إنجازها عبر بوابة إلكترونية، إلى جانب أدوات القرصنة، والأسلحة الإلكترونية، فقد هدفت هذه المعاهدة إلى تحريك التعاون الدولي في مواجهة المخاطر الإلكترونية، وتبادل المعلومات في هذا الشأن وذلك عبر طرح عدة قوانين تحكم هذه العملية أو الشراكة،[181] ولكن هذه العملية لازالت تواجه عدة صعوبات رغم ازدياد عدد الدول المنضمين للمعاهدة مثل اليابان، وأفضل مثالا على ذلك هو قيام مركز المعلومات للخصوصية الإلكترونية (Electronic Privacy Information Center) وهو بمثابة مجموعة بحثية أمريكية للمصلحة العامة (Public Interest Research Group)، بتسليط الضوء على هذه المعاهدة للرأي العام، كما إرسال رسالة لمجلس الشيوخ الأمريكي لنبذ مثل هذا التعاون لأسباب تتعلق بالدستور الأمريكي، وقضايا الخصوصية، والتجسس، وحقوق الإنسان.[182]

إذ نظرنا إلى هذه المبادرة، ورغم أن تعالج قضايا إلكترونية واسعة، إلا أنه يمكننا أن نرى أن لا تتعاطى مع الأمن الإلكتروني، والأسلحة الإلكتروني، كوسيلة للصراع، والحروب في العلاقات الدولية، فإذا نظرنا اعمق يمكننا أن نجد أن معظم القوانين التي تعتمدها، لديها طابع جنائي خاصة بالأفراد، وتسيير المصالح القانونية للمؤسسات، والمواطنين، والتعاون الجنائي فيما يخص الأدلة، ومكافحة التطرف ، فهذه المبادرة مربوطة بالفواعل الرسمية فقط، وسنفهم جيدا، لو أن فواعل غير رسمية مثل ما ذكرنا في

---

(180) Attila Fernc Varga, "Rules of Engagements and International humanitarian Law," in **LAW**, No 1, Volume 11(2012), pp. 1-11.
(181) Council of Europe, **Convention on Cybercrime**, Budapest, November, 2001, pp. 1-22.
(182) Declan McCullagh, "Senate ratifies controversial cybercrime treaty", in: ***http://goo.gl/m900FO***, (Friday, May 20, 2016).

قضايا الحرب التشفيرية، ستحاول العمل جاهدا على صد هيمنة الدولة ورقابة الدولة، وسيطرتها على العالم الافتراضي باي طريقة ممكنة.

بالإضافة إلى هذا يمكننا القول أن مثل هذه المبادرات لا تعالج جوهر الصراع الإلكتروني الدولي، وهذا ما عبر عليه العديد من الباحثين، الذي يرون أن معالجة الأمن الإلكتروني، خاصة في العصر الحالي، يجب أن يكون من منطلق القانون الدولي، كون الأمن الإلكتروني أصبح في وسط معادلة الهيمنة في العلاقات الدولية، فبغض النظر على أن معظم الأسلحة أصبحت تستند إلى قاعدة إلكترونية مسؤولة على توظيفها وطريقة عملها، إلا انه من جانب آخر، أصبحت توظف الأسلحة الإلكترونية أيضا لإلحاق الضرر المادي، والجسدي، والمعنوي.

فالطابع العسكري الذي أصبح إليه الأمن الإلكتروني، والصراع الإلكتروني بصفة عامة، دفع بالكثير إلى طرح الفكرة التي تقول، على أن قضايا الأمن الإلكتروني، والحروب الإلكتروني، يجب ضبطها، وإدماجها مباشرة ضمن اتفاقيات جينيف، فقد تكلم قائد القيادة الإلكترونية للولايات المتحدة الأمريكية، ومدير وكالة الأمن القومي **مايكل روجرز** (Michael S. Rogers) على أن الأسلحة السبرانية تمثل الجيل القادم من الحروب، وصرح على أنه:[183]

> "**يجب تذكر أن أي شيء نقوم به في الساحة الافتراضية ... يجب أن يتوافق وقوانين النزاعات المعمول بها. فأي رد من طرفنا يجب أن يتوافق ودرجة هجوم العدو، يجب أن نتعامل وفق كامل المعايير التي قمنا بإنشائها مع مرور الوقت، ولا أظن أن الفضاء السبراني يشكل فرقا في الأمر**".

فمن المتعارف عليه، أن الأسلحة الكيماوية تم تحريمها أثناء فترة الحربين، وهي مجسدة في اتفاقيات جينيف، لكن هذا الأمر لم يمنع العديد من الدول من امتلاك هذا النوع من الأسلحة، لذا ووفق هذا، يُرى أنه من الصعب جدا، تقنين الأسلحة الإلكترونية، وضبطها، ومراقبتها، ولكن يمكن أن تجسد كقوانين ستساهم في

(183) Franz-Stefan Gady, "A Geneva Convention for Cyberspace?," in: ***http://goo.gl/PFRRrq***, (Friday, May 20, 2016).

التدخل الدولي في مرحلة ما، أو كورقة ضغط كما حصل في سورية فيما يخص مخزون الأسلحة الكيميائية لديها.[184]

إذ نظرنا إلى قوانين جينيف، والبرتوكولات التي أتت بعدها، يمكننا أن نقول أن أقرب بند يمكن أن يضم الأسلحة الإلكترونية، هو البند 36 من البروتوكول الأول 1977 الذي ذكرناه سابقا، وهذه المادة تنص على أن أي سلاح مستقبلي يتم اختراعه من قبل الدول، يجب أن يتوافق، ويحترم، القوانين الإنسانية الدولية، وتم طرح سنة 2003 في المؤتمر العالمي للصليب الأحمر إلى ضرورة التعامل ومعالجة الأسلحة الجديدة التي بدأت تظهر، كما الأساليب الجديدة في ممارسة الحرب بطريقة بين تخصصية وذلك من أجل ضمان أن الحماية القانونية، لا يتم تجاوزها بالتقدم التقني.[185]

لقد راينا أنه كيف يمكن لقوانين الحرب القديمة أن تؤثر في العمليات القتالية التي تحدث في العالم حاليا،[186] لكن الأمن الإلكتروني، وقضايا الحرب السبرانية أصبحت تشكل تحديا فعليا لقوانين الحرب،[187] فالأمن الإلكتروني أصبح يطرح أسئلة معقدة يصعب الإجابة عليها بسهولة، خاصة تلك التي لها علاقة بموضع الأسلحة الإلكترونية من القوانين الدولية، قضايا تصنيفها على أنها أسلحة دمار شامل أو لا، إذ كيف يمكن تقنين حرب يمكن للجميع أن يشارك فيها، فميزة الأمن الإلكتروني، وصراع الهيمنة العالمي، هي أن كل شخص يمكنه أن يشارك، فكيف يتم تحديد الأهداف المدنية؟، وكيف يتم تحديد العدو؟، وكيف نتعامل وفق قواعد الاشتباك ؟. يمكننا أن نجد العديد من القوانين العامة مثل البند 39 الذي ذكرناه، والبند 49 من نفس البروتوكول، والذي يُعنى بأي شيء يمكنه أن يسبب ضررا

---

(184) Chris Weigant, "We Need a Geneva Convention on Cyber Warfare," in: ***http://goo.gl/cMcxKJ***, (Friday, May 20, 2016).

(185) International Committee of the Red Cross, ***Cyberwarfare and international humanitarian law: The ICRC's position***, June, 2013, pp. 1-4.

(186) Erki Kodar, "Applying the Law of Armed Conflict to Cyber Attacks," in **ENDC Proceedings**, Volume 15, (2012), pp. 107-132.

(187) D. Hollis, "Why States Need an International Law for Information Operations," in **Lewis & Clark Law Review**, volume 11(2007), p. 1023.

جسديا أو معنويا أو ماديا،[188] بالإضافة إلى البند 52 الذي يعني بعدم استهداف المرافق المدنية والاقتصادية بطريقة تقليدية أو افتراضية وفقا للإسقاط التطبيقي للبند؛[189] لكن في الحقيقة، توضح لنا هذه المحاولات التخبط الموجود في قضايا الأمن الإلكتروني في القوانين الدولية، فمعظم المحاولات القانونية غير دقيقة، وقد تم وضعها لتغطي أغراض غير القضايا الإلكترونية، مثل محاولة تطبيق نفس قوانين التي تعنى بالأسلحة العادية على الأسلحة الإلكترونية، أو التأثير الذي تحدثه هذه الأسلحة، بالإضافة إلى هذا فالقوانين الدولية تعنى أكثر بالفواعل الرسمية أثناء الحرب، لكننا نعرف جيدا أن الأمن الإلكتروني، والصراع الإلكتروني العالمي، هو صراع شامل، والجميع معني بذلك.

إن طبيعة النموذج التقليدي للحرب والأمن، سهل من عمل القانون الدولي، وذلك لارتباطه أكثر بالفواعل الرسمية، لأسباب تتعلق باحتكار القوة، والسياسة، والإمكانيات. الأمر الذي أصبح أقل أهمية في عصر الأمن الإلكتروني، ويبدو أن القانون الدولي بدا يعاني من التعقيد الكبير الذي جاء به هذا العصر، فمعظم محاولات تأطير الأمن الإلكتروني، نرى أنها لا تأخذ بلامركزية القوة والأمن في العصر الحالي، ولعل طبيعة الجهات المعنية بوضع هذه القوانين أثر على المنظور الذي يجب أن يكون أو يسود.

(188) Erki Kodar, **op, cit.**
(189) Loc. Cit.

2.3 أساليب وآليات محاربة الهيمنة في العلاقات الدولية

التكلم على محاربة الهيمنة في العلاقات الدولية، مربوط بالتكلم على الصراع الدولي بشكل عام، وفي هذا الموضوع، سندرس أكثر الأساليب التي لها علاقة بالأمن الإلكتروني، والوسائل التي تستخدمها مختلف الأطراف من أجل تحقيق مصالحها عبر البوابة الإلكترونية، فالأساليب التي تعتمد في الصراع الدولي، والتي تستند إلى قاعدة إلكترونية، لا يمكن إحصائها جميعا، وذلك لتعددها، ولإمكانية تغييرها وقولبتها وفقا لرغبات محددة، ويمكن النظر إلى الأمر كذلك الشخص الذي يصنع سلاحا، أو قطعة سلاح وفقا لمتطلبات قتالية معينة، كذلك يجب معرفة أن الصراع الإلكتروني الدولي أيضا يختلف باختلاف الإمكانيات المادية التي يمكن أن تسخرها أي جهة من اجل صنع الأسلحة، أو القيام بهجمات معينة، فهذه العلاقة بين الإمكانيات ونوع الهجوم يمكن أيضا فهمها من خلال القضايا التي تهدف إليها كل جهة، كون بعض الهجمات التي يمكن أن تسبب أضرار للبنى التحتية للدول، ستحتاج إلى قاعدة هيكلية لا يمكن أن تتوفر للجميع.

ولهذا سنعالج هذا الموضع بالتطرق، أو بتقسيم أهم الفواعل، أو اهم العناوين التي يمكننا في ضمنها أن ندرج مختلف الجهات التي تتصارع في العلاقات الدولية، وذلك من اجل جمعها وتبويبها قدر الإمكان، ولكن يجب معرفة أن هذا التنصيف لا يعد نهائيا، بل وضع فقط من اجل ضبط الفواعل، وأهم الاتجاهات، فالأمن الإلكتروني، وقضايا الصراع العالمي، أعطت إمكانية للفرد الواحد بان يكون فاعل، وذلك عبر قيامه باي شيء بدافع الضغط أو تحقيق المكاسب عبر أدوات مختلفة جاهزة موجودة على الشبكة العالمية.

2.3.0 الدولة والقوى الإلكترونية

الذي لا شك فيه، هو أن الدولة حاليا أصبحت على دراية جيدة بالمخاطر التكنولوجية، خاصة منها التي تتعلق بالأمن الإلكتروني، وأمن المعلومات، ولن نبتعد كثيرا عن الموضوع إذا قلنا أن رؤية التطبيقات العسكرية لأي تقانة جديدة يعد أمرا لا يمكن الهروب منه، فحاليا، وفي مختلف الجيوش المحدثة، والتي تعتمد على أنظمة الاتصالات، والرادارات، وأي قاعدة إلكترونية، نرى أنها تعتمد على فرق خاصة، وفي بعض الأحيان على وكالات أو وحدات بأكملها في الجيش، متخصصة في الحرب الإلكترونية، والدفاع عن مصالح البلاد.

يمكننا أن نرى الأهمية الذي أصبح يشكله الأمن الإلكتروني بالنسبة للدولة في خطاب الرئيس الأمريكي الحالي **باراك حسين أوباما** (Barak Hussein Obama) في قمة الأمن الإلكتروني فبراير 2015، حيث قال:[190]

> ***"إن أمن الولايات المتحدة الأمريكية، واستقرارها الاقتصادي، وحرياتنا الشخصية تعتمد على مدى قدرتنا في تامين الفضاء الإلكتروني، وتأمين شبكة عالمية مفتوحة، ومستقرة، ومؤمنة. فهياكلنا الحيوية لازالت معرضة للتهديد من قبل المخاطر الإلكترونية، كما أن اقتصادنا يعاني من الأضرار جراء سرقة الملكية الفكرية. لهذا فالمخاطر موجودة فعلا وهي في تطور بطريقة مستقرة ومستمرة، أنا أؤمن أنه إذا تمكنا من ضبط هذا المجال بشكل فعال، سنتمكن من تأمين الشبكة العالمية، وجعلها أحد أهم محركات النمو الاقتصادي، ووسائل التبادل الفكري".***

فالدولة تعد اكبر فاعل في الفضاء الإلكتروني والصراع الإلكتروني، وذلك يرجع للإمكانيات التي يمكن أن تسخرها في هذا الشأن، ولكن مثل عمليات الصيد، كلما كان الهدف اكبر، أصبح من السهل على الصياد ضرب فريسته، فالولايات المتحدة الأمريكية مثلا، تتلقى 550.000 الف هجوم في الأسبوع، أي ما يفوق 25.000.000 هجوم في السنة، كما أن الهجوم على المواقع الحكومية تضاعف من 31.000 سنة 2012 إلى أكثر من 60.000 سنة 2014، فالهجمات الإلكترونية في تزايد مثل الطاعون،[191] ولهذا هناك من يقسم الهجمات التي للدول إلى ثلاثة مستويات، وكل مستوى يوضح مدى تجاوب الدولة مع هذا التعديد من أجل حماية نفسها، لأنه من المتحيل أن تتجاوب الدولة مع 550.000 الف هجوم في الأسبوع، لهذا يتم تقسيم أنواع الهجمات، وتقسم صلاحيات التدخل على السلطات المختصة، وطبعا الهجمات من المستوى الثالث والتي تشير إلى إمكانيات كبيرة للعدو وأهداف تتعدد من تهديدات للثروة المائية، إلى البنى التحتية الحيوية للبلاد، ستتطلب تدخل على نطاق أوسع من قبل الدولة عكس أن يكون الهجوم من المستوى الأول بسبب عمليات احتيال إلكترونية بسيطة مثلا، والتي في هذه الحالة لن نرى سوى تدخل سلطات محلية متخصصة.[192]

---

[190] Joseph N. Pelton, Indu B. Singh, **Digital Defense, a Cybersecurity Primer** (Switzerland: published by Springer International Publishing, the first edition, 2015), p. vii.
[191] ***Ibid***, p. ix.
[192] ***Ibid***, pp. 6-21.

تجدر الإشارة هنا أنه لا يجب اعتبار أن كل الدول لديها نفس القدرات، ولكن يعد الأمر معضلة حقيقة لما نرى دولة مثل الولايات المتحدة الأمريكية عاجزة أمام هذا المجال، وتعرض كل سنة ارقما تتعدى آلاف ملايين الدولارات كخسائر جراء المخاطر والتهديدات الإلكترونية. ولهذا فالدولة تسعى دائما كي تكون قوة إلكترونية في المجتمع الدولي، فالقوة الإلكترونية، مثل ما هو الحال مع الإلكترونية مثلا، فهي تشير إلى قدرة الدولة على التأثير على جهة أخرى في العالم الرقمي، أكان الأمر ضد دولة معينة، أو ضد فواعل غير رسمية. (193)

فالدولة يمكنها أن تعتمد على العديد من الوسائل كما التي وضحناها سابقا في الحرب المعلوماتية أو التشفيرية، وذلك من أجل التجسس، أو من اجل تنفيذ عمليات عسكرية إلكتروني، والتي ستحتاج عدد كبير من الخبراء والمتخصصين من أجل تنفيذ هذه العمليات، كما التكنولوجية القاعدة التي لها علاقة مباشرة بالهياكل، والموارد المالية، إلى جانب الإرادة، أو القرارات السياسة، فالدولة عكس بقية الفواعل الغير رسمي، لديها هيكلية معينة في شن الحروب، وأي قرار تنفيذ أي عملية يجب أن يكون من أشخاص معينين لديهم صلاحية القيام بذلك. ولهذا نجد أن عالم السياسة الأمريكي بيتر سينجار (Peter W. Singer) والذي يعمل في منصب المدير لمركز القرن 21 للدراسات الأمنية حيث صرح بأن:(194)

> ***"هناك حوالي 100 دولة حاليا تعمل على بناء قدراتها الإلكترونية العسكرية، ومن بين هذه الدول، هناك 20 دولة يمكن اعتبارها كلاعب جاد وفعال في العلاقات الدولية، مع عدد اقل من الدول التي بإمكانها شن حملات هجوم إلكتروني على نطاق واسع".***

بالإضافة إلى هذا فإن الأهداف التي تسعى إليها الدولة عبر استخدام الفضاء الإلكتروني، يمكن أن تتعدد كثيرا، فالدولة يمكنها أن تستغل الفضاء الإلكتروني لاكتساب بعض المصالح السياسية عبر استخدام أقل الإمكانيات الممكنة، ويمكن أن يكون للأمر علاقة بالجوسسة كما ذكرنا، أو جمع المعلومات، أو استهداف شركات محددة، فالدولة بإمكانها استهداف القطاع الخاص لدولة أخرى. افضل مثال على ذلك هي العملية التي أمسيت بعملية أورورا (Operation Aurora) والتي تعبر على قيام الصين حسب الولايات المتحدة الأمريكية بهجومات على نطاق واسع على الشركات والمصالح الإلكترونية

---

(193) Chris C. Demchak, **Wars of Disurpation and Resilience** (Athen: published by The University of Georgia, the first edition, 2011), p. ix.

(194) Steve Ranger, "Organized cybercrime groups are now as powerful as nations," in: ***http://goo.gl/HiywTa***, (Saturday, May 28, 2016).

للعديد من الشركات مثل ما حدث مع شركة غوغل التي تم اختراق العديد من الحسابات التي تبين فيما بعد أنها تنتمي إلى العديد من النشطاء الحقوقيين في الصين.[195]

يجب أن نعرف هنا أن أساليب محاربة الهيمنة، يمكن أن يكون عبر الهجوم على مختلف التهديدات المحتملة، أو وضع آليات للدفاع ضد مختلف التهديدات، وهذا ما يمكننا رؤيته في أصبح يسمى حاليا بالأحلاف السيبرية (Cyber Alliance)؛ فهذا النوع من الأحلاف يعبر على مجموعة من الأنماط الرسمية النابعة عن مجموعة من الاتفاقيات الصريحة بين الجهات الفاعلة الدولية أو الغير دولية، والتي سينتج عن هذه العملية مجموعة من الالتزامات المتبادلة في الحقل الذي له علاقة خاصة بالدفاع الإلكتروني، ويمكننا فهم ذلك من خلال البحث في أنواع هذه الأحلاف والأهداف التي تسعى إليها، ولهذا يمكن تقسيم الأحلاف الإلكترونية إلى:[196]

1. **الأحلاف التقليدية:**

ويعد حلف الناتو أفضل نموذج على ذلك، حيث دفع عجز حلف الناتو في مواجهة الهجمات الإلكترونية على إيستونيا وجورجيا إلى تكوين وحدة الدفاع الإلكتروني، وعمل على تطوير المفهوم الاستراتيجي للحلف حيث اصبح الفضاء الإلكتروني مصرحا لعمليات الحلف. كما عمل أيضا على تطوير قدراته في الإسناد والدعم للدول الحليفة عند تعرضها للهجوم.

2. **التحالف بين دول وشركات التكنولوجيا:**

وأفضل مثالا على ذلك هو التحالف في مجال الأمن الإلكتروني الذي حصل سنة 2010 بين دائرتي الدفاع والأمن الداخلي الأمريكية، وكبريات الشركات الصناعية الخاصة، ويقوم هذا النوع من التحالف على إشراك أصحاب المصالح كحليف قوي لتحقيق الأمن الإلكتروني.

3. **التحالف بين شركات التكنولوجيا:**

ويعبر على مجموعة من التحالفات التي يمكن أن تحد بين مجموعة من الشركات بهدف تقاسم المعرفة والخبرة، وتطوير عام للأمن الإلكتروني.

4. **التحالف بين المنظمات الدولية وشركات التكنولوجيا:**

---

[195] Andress Jason, Winterfeld Steve, **Cyber Warfare: Techniques, Tactics and Tools for Security Practitioner** (Online: published by Syngress, the 2nd edition, 2013), p. 14.

[196] دعاء الجهيني، "الأحلاف الإلكترونية،" في ***اتجاهات الأحداث***، العدد 6 (يناير، 2015)، ص ص. 11–13.

ومن أمثلة ذلك قيام حلف الناتو من خلال وحدة الدفاع الإلكتروني، التي تم إنشاؤها سنة 2007، بتغيير استراتيجيته من مجرد الاكتفاء بالدول المنظمة للحلف والمعنية بتحقيق الأمن الإلكتروني لها، ليضم جهات فاعلة من غير أعضائه الطبيعيين من الدول، وذلك عبر تعزيز الشراكة والتعاون مع الشركات العالمية وكذلك توسيع نطاق التحالف لتشمل دول في منطقة الشرق الأوسط.

يمكن أن نفهم من هنا وجود أخطار عديدة تواجه الدولة، كم الوسائل أيضا التي تستخدم في هذا التخبط من أجل الهيمنة وتأمين الذات، فهناك العديد من الأحداث التي كشفت الصراعات الإلكترونية، ولعل من ذلك الهجمات الإلكترونية الأخيرة على سوني، ومن قبله فيروس ستوكسنت الذي استهدف البرنامج النووي الإيراني، فضلا عن إتهام الولايات المتحدة الأمريكية المستمر للصين بالتجسس الاقتصادي، والصناعي، والقرصنة المعلوماتية، بالإضافة إلى تسريبات ويكيليكس،[197] ومخاطر اقتصادية جد مخيفة ومدمرة مثل ما هو الحال مع ما يسمى *بالانهيار الفائق السرعة(Flash Crash).

فالتحالفات ورغم أهميتها، إلا أن الثقة دائما تبقى المشكلة الأكبر في أي تحالف إلكتروني يدعوا إلى تبادل المعلومات، فالطرق التي تستخدمها الدولة كما رأينا تعد عديدة، ولا حدود لها، والبعض من هذه الطرق يمكننا حتى إيجادها عند

---

[197] نفس المكان.

- انهيار الفائق السرعة(Flash Crash): انهيارات حدثت عدة مرات في البورصات التي تعتمد على التبادل الفائق السرعة (High-frequency trading) الأمر الذي يؤدي إلى خسائر فائقة في أجزاء صغيرة من الثانية، لأسباب مجهولة في بعض الأحيان، لهذا هناك تبادل مستمر في الاتهامات، خاصة ضد الجهات الكبرى التي لديها تأثير في السوق.

الفواعل الغير رسمية، ولكن كما عرضت في الجزء الأول من هذه الدراسة، من المستحيل أن تؤمن الدولة نفسها بشكل كامل، لهذا فهي تعتمد على الذهنية التقليدية القائمة على الاستعداد والهجوم لحماية نفسها، أو اللعب على ورقة الهجوم من أجل كبح تقدم العدو أو تحقيق أية مصالح ممكنة.

2.3.1 الإرهاب الإلكتروني

يعد استخدام الحركات الإرهابية للمجال الإلكتروني من اجل تحقيق المصالح التي تهدف إليها أمرا متوقعا، خاصة في ظل العولمة التي دعها التطور التقني المتزايد إلى ابعد حد يمكن تصوره، ولهذا فالجماعات الإرهابية، بغض النظر عن تحديد ماهية الجماعة الإرهابية، فهي تستخدم كل الوسائل من أجل التجنيد، أو جمع الأموال، أو التهديد، أو مختلف الوسائل، والمصالح التي يمكنها تمريرها عبر استخدام البوابة الإلكترونية.

إذا كان الإرهاب يمكن التعبير عليه على انه قيام منظمة معينة بترعيب الناس، وذلك لغرض تحقيق مكاسب سياسية معينة،[198] يمكن في المقابل النظر إلى الإرهاب الإلكتروني على أنه استخدام للشبكة العنكبوتية، وإرسال المعلومات، والتهديدات، والقيام بعمليات تدميرية بهدف خلق الشعور بالخوف، وترك الانطباع النفسي عند الأشخاص، مثل الحرب الدعائية.[199] فالضغوطات الكبير على الجماعات الإرهابية وهيمنة الدولة على الاتصالات الرسمية، تجعل من الفضاء الإلكتروني وسيلة فعالة من اجل الالتفاف على رقابة الدولة، فالفضاء الإلكتروني يسهل عملية التجنيد، كما يسهل عمليات الترويع، ونشر الكراهية بين الأشخاص، ففي الوضع الحالي، يمثل الفضاء الإلكتروني مكان ممتازا لانتعاش الحركات الإرهابية.[200]

يمكننا أيضا أن نقول أن الإرهاب الإلكتروني أصبح لديه الآن قوة كبيرة على التأثير على الرأي الهام، وتحفيز الشعور العنصري والكراهية، فقوة الإرهاب الإلكتروني تكمن في الوسائل العديدة والمتنوعة التي يمكنه استعمالها من اجل تحقيق مصالحه، والسعي وراء الأهداف التي يريدها؛ مثل استخدام

---

[198] Sheldon JB, "Sate of the Art: Attacker and Targets in Cyberspace," in ***the Journal of Military and Strategic Studies***, Volume 12 (February, 2012), pp. 1-19.

[199] Jonalan Brickey. "Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace,"in: ***https://goo.gl/Tu09Ml***, (Saturday, May 28, 2016).

[200] Rudner M, "Cyber threats to critical national Infrastructure: An intelligence challenge," in ***International Journal of Intelligence and Counterintelligence***, Volume 26, (Marsh, 2013), pp. 453-481.

القرصنة، والتجسس، والاحتيال، وكل وسيلة ذكرناها سابقا وتدخل في إطار الإكراه الإلكترون. بالإضافة إلى هذا، فإن بروز بعد التكنولوجيات الجديد والظواهر الجديدة ساهم بشكل كبير جدا في انتعاش الحركات الإرهابية على الأرض، وذلك عبر توفير وسائل جديدة لتنقل الأموال التي يمكن تتبعها. فقد أصبحت معظم الحركات الإرهابية تستخدم وتستثمر في عملة البيتكوين (Bitcoin)، التي تعد أول عملة معمات ومشفرة (Cryptocurrency) ولا مركزية، ويمكن تبادلها بين الأشخاص، واستخدامها لشراء المعدات، أو تحويلها مقابل مال حقيقي متداول؛ فإذا كان الشخص يخزن أمواله في البنوك، [201] فإن البيكوين يخزن إلكترونيا، ويمكن لأي شخص أن يحمل **مليارات الدولارات في قرص صلب صغير يضعه في جيبه** ويتنقل بها من بلد لآخر بدون أن يعرف أحد، الأمر الذي جعل من البيتكوين وسيلة ممتازة لنقل الأموال، وتبييضها.

الصورة رقم: 2.0

قطع معدنية، تمثل قيمة ثابتة لعملة البيتكوين الافتراضية، كما رمز العملة أيضا. [202]

كما جعل من هذه العملة أيضا وسيلة ممتازة لمحاربة هيمنة الدولة على الأموال وتنقلها، يمكننا أن نرى هنا تزعزع فعلي لهيمنة الدولة والقوى الدولية على تنقل الأموال، والسيطرة عليها، أو مراقبتها، الأمر الذي جعل مثل هذه التكنولوجيات الجديد، أحد أهم الأساليب المتبعة في الصراع الدولي القائم، فمن غير المستبعد أن تكون العديد من الحكومات قد باشرت في الاستثمار في هذا النوع من العملات، خاصة وأنه يمكن التنقيب عليها عبر استخدام الحواسيب الفائقة، لهذا لا تعد هذه العملة وسيلة في أيادي الجماعات

[201] Jean-Paul Delahaye, "Le Bitcoin, première crypto-monnaie," dans ***Bulletin de la société informatique de France***, No 4 (Octobre, 2014), pp. 67-104.
[202] A metal representation of the Bitcoin Currency, in: ***http://goo.gl/y4xnkQ***, (Saturday, May 28, 2016).

الإرهابية فقط، بل في يد الجميع، الدولة، والجماعات الإرهابية، والنشطاء الإلكترونيين، واي شخص يمكنه الولوج إلى الشبكة العنكبوتية، أو لديه حاسوب قوي كفاية لينقب على هذه العملة؛ وقد أصبحت هذه العملة مع مرور الوقت رمزا للتحرر، والمقاومة، ومخالفة الأنظمة القائمة.

2.3.2 الجريمة المنظمة الإلكترونية

يمكن النظر إلى الجريم المنظمة الإلكترونية على أنها تلك الحلقة التي تقوم بربط الدولة، والإرهاب الإلكتروني، والهاكتيفيزم؛ فالجماعات الإرهابية يمكنها الاعتماد على خدمات الجريمة المنظمة من اجل تحقيق أهداف سياسية معينة، لكن الجريمة الإلكترونية في المقابل، فإنها تركز أكثر على تحقيق الأرباح المادية وراء العمليات التي تقوم بها، فرغم أن مصالح المنظمات الإجرامية يمكنها أن تتعدد، إلا أن الطابع السياسي للعمليات التي تقوم بها لا يعد حاضرا، حتى وإن تم ذلك، سيكون في سياق تحقيق أرباح ومصالح معينة على حساب مصالح سياسية سيستفيد منها الطرف الآخر.

فالجريمة المنظمة الإلكتروني، تدخل في سياق ما يسمى حاليا، بالجرائم المستحدثة، أو جرائم التقنية العالية (High-technology crimes)، [203] فالجريمة المنظمة تعتمد على تنظيمها الحالي، وهي تميل أكثر للضربات الجراحية من اجل تحقيق أهدافها، وذلك عبر استخدام مختلف الوسائل المتوفر مثل ما هو الحال مع هجوم حجب الخدمات، فالجريمة المنظمة تعمل كمرتزقة، وسيط، وهدفها الأساسي هو استغلال الفرص التي أتاحتها التكنولوجية من اجل تمديد وتنويع أنشطتهم الإجرامية.

بالإضافة إلى هذا، فالجريمة الإلكترونية، كما قلت تقوم على علاقات معقدة قائمة على الفرصة المتاحة من اجل تحقيق الأرباح، والأشخاص وراء هذا النوع من الجرائم يعرفون في العادة أين تمكن نقاط ضعف الدولة، أو الجهة المستهدفة، فملا يمكن لقرصان معين أن يقوم بسرقة معلومات اقتصادية مهمة من شركة معينة؛ هنا لديه خيار استخدام هذه المعلومات المهمة لصالحه، أو لديه خيار آخر وهو أن يقوم ببيع هذه المعلومات لأشخاص متخصصين في تحليل المعلومات، أو من مصلحتهم الحصول على

---

[203] محمد أمين البشري، ***التحقيق في الجرائم المستحدثة*** (الرياض: نشر من قبل جامعة نايف للعلوم التكنولوجية، الطبعة الأولى، 2004)، ص. 85.

هذا النوع من المعلومات، أو حتى القيام برشوة أحد الموظفين البنكيين من أجل تبيض الأموال، أو استخدام البطاقات البنكية التي تم قرصنتها. [204]

كما أن الجريمة الإلكترونية أيضا معنية بقضايا العملات الإلكترونية، وأي شيء يمكن أن يحقق الأرباح، وربما يمكننا أن نرى نوع من الأنماط هنا، وخاصة التي تتعلق باستغلال الفرص، فبعد سقوط الاتحاد السوفييت، حاولت العديد من المنظمات الإجرامية شراء رؤوس نووية من السوق السوداء، وذلك من أجل بيعها فيما بعد إلى الذي سيدفع أكثر، كذلك الجريمة المنظمة الإلكترونية، فهي تعبر عن مجمل التعاملات والعمليات التي تهدف إلى تحقيق الربح، مستقلتا بذلك الضعف الكبير للدولة في العالم الافتراضي، والتراجع الكبير في هيمنة الدول على حدودها وعلى مصادر الربح التي تشترط عمليات رقابية لها صلة بالضريبة ومكافحة تهريب وتبييض الأموال.

فقد أثبتت مثل هذه القدرات، وكذا الأضرار الكبيرة التي تسببها مثل هذه الجماعات، على أنه هناك العديد من مجموعات الجريمة الإلكترونية المنظمة التي وصلت إلى درجة عالية جد من التطور تنافس بها حتى الدول القائمة بذاتها، فقد اصبح بمقدور هذه الجماعات بناء أنظمة معقدة تهدف إلى سرقة الأموال وجمع المعلومات وسرقة الملكية الفكرية الأمر الذي يسبب للاقتصاد العالمي ما يفوق 360 مليار دولار من الخسائر.[205] كمثال على ذلك، نجد أنه في سنة 2014 قامة منظمة إجرامية روسية، بسرقة بطاقات الائتمان، والتي تضمنت بيانات 1.2 مليار مستخدم، وكلمات السر لأكثر من 500 مليون بريد إلكتروني، ثم قامت هذه الجماعة ببيع هذه المعلومات في السوق السوداء إلى عصابات أخرى التي استغلت هذه البيانات للقيام بمختلف أنواع الهجمات، وتثبيت الدود الإلكتروني في عدة أماكن على الشبكة الأمر الذي أدى بالمستخدم العادي مثلا إلى تحميل أشياء مفخخة من غير علمه.[206]

يمكننا أن نعرف من هنا، أن ما تمثله الجريمة المنظمة الإلكترونية، هو وجح جديد لهذا العصر، فمن المتعارف في عالم الأمن الإلكتروني أن الحماية لا تدوم للأبعد، خاصة فيما يتعلق بالألعاب الإلكتروني، والتي يتم قرصنها بشكل سريع، ويتم نشرها على الشبكة من أجل التحميل المجاني، والأمر لا يتعلق فقط بالحماية

---

[204] Steve Ranger, "Organised cybercrime groups are now as powerful as nations," in: ***http://goo.gl/3Kqi9X***, (Saturday, May 28, 2016).
[205] Loc. Cit.
[206] Hold Security, "YOU HAVE BEEN HACKED!," in: ***http://goo.gl/Y8Jq3m***, (Saturday, May 28, 2016).

الإلكتروني، بل بكل ما له علاقة أو موجود على الشبكة؛ يبدو أنه مثل ما تأثرت بقي المجالات الإنسانية بعملية الرقمنة التي حصلت، نرى في المقابل استغلال الجريمة المنظمة لهذا الأمر في صالحها، بل سيكون في صالحها لمدة طويلة، ففي العالم الافتراضي، لا يمكن لأحد أن يتكلم من منطلق الأقوى أو المهيمن، والدولة عاجزة أمام هذا الأمر، آلاف الجرائم ولكن بدون أدلة، أضرار أصبحت تعرض بمليارات الدولارات، وسببها حفنة صغيرة من الأشخاص المدربين.

2.3.3 الهاكتيفيزم

قبل التكلم على الهاكتيفيزم، يجب القول، أن التقانة، وتطور التكنولوجيا، كما اختراع الشبكة العنكبوتية العالمية، وتوفرها أكثر فأكثر للسكان في الأرض، جعل من الشبكة كعالم موازي تتضارب فيه الأفكار والمصالح والأهداف، ولكن الأهم هنا، هو أن الشبكة العنكبوتية العالمية، خلقت ثقافة واحدة يتشارك فيها الجميع، فالعالم الافتراضي وبحكم التفاعل الطويل بين مختلف المجتمعات ساهم في خلق وعي بالقضايا التي تهم الإنسانية، واصبح المجتمع الإلكتروني يعمل في العديد من الأحيان من أجل التأثير على المخرجات السياسية، فالهاكتيفيزم يشير إلى عمل النشطاء التقليدي ولكن بطريقة إلكترونية، وهو يهدف فقط إلى القضايا التي تهم الإنسانية وحرية التعبير بشكل عام، ولا علاقة له بالربح المادي.

وهذا الوعي جسد في العديد من المرات من قبل المجتمع الإلكتروني، وبرهن فعلا على أن المجتمع الإلكتروني العالمي يمكنه أن يعمل من أجل القضايا التي تهتم بالإنسان، ففي سنة 1989، أعلنت مجموعة القراصنة المسمات بفيلق الأرض السفلى (Legions of the Underground)، والموجودة في الولايات المتحدة الأمريكية الحرب الإلكترونية على العراق والصين، وذلك حسبهم لأسباب تتعلق بحقوق الإنسان، وذلك عبر قطع قدرة هذه الدول على الولوج إلى الشبكة العنكبوتية العالمية ؛ بعد أسبوع من هذا الإعلان أقيم تحالف كبير من القراصنة في العالم، ومن بينهم يمكن أن نجد طائفة البقرة الميتة (Cult of the Dead Cow)، و(L0pht) بالإضافة إلى نادي فوضى الحاسوب الموجود في ألمانيا (Chaos Computer Club)، ومجموعة (mags 2600)، و(Phrack) إلى جانب العديد من الفرق الأخرى،

هذا التحاف نشر بيان طويل واضح اللهجة يعارض فيها فيلق الأرض السفلى، [207] وأهم ما جاء في خلاصة البيان هو ما يلي:[208]

> ***"الموقعين على هذا الإعلان ينادون على معارضة أي عملية تهدف إلى إلحاق الضرر بالهياكل القاعدية للمعلومات لأي دولة. لا تدعموا أي فعل يدخل في نطاق الحرب الإلكترونية. حافظوا على شبكات الاتصال بشكل حي، لأنها تمثل العصب الرئيسي للتطور الإنساني".***

مثل هذه المبادرة توضح بشكل كامل، مغزى المجتمع الإلكتروني والهاكتيفيزم، فالهاكتيفيزم والذي يعد العضو أوميجا (Omega) من مجموعة طائفة البقرة الميتة أول من قام بقولبته(Hacktivismo-Hacktivismo) سنة 1996، [209] اصبح يعبر حاليا على الأهداف الإنسانية العليا، والعمل على التأثير على القرارات السياسة للقادة، أو الاحتجاج عبر الاختراق.

يجب أن نعرف أيضا أن العمليات التي تهدف إلى محاربة الهيمنة ومصالح الدول الكبرى كانت موجودة حتى قبل بروز هذا المصطلح طبعا، وغير مثالا على ذلك هو قيام مجموعة من القراصنة سنة 1989 بعملية اختراق ضد قسم الأبحاث المتعلقة بالطاقة النووية الخاص بوكالة ناسا الأمريكية، إذ أنه عندما حاول الموظفين دخول الحواسيب والشبكة، لم يستطيعوا ذلك، ووجدوا كلمة (WANKed) موضوعة بشكل ساخر، والتي كانت تشير إلى (Worms Against Nuclear Killers)، هذه الدودة تم وضعها من قبل قرصان صغير من أستراليا، وذلك احتجاجا على القضايا التي لها علاقة بالتجارب النووية؛ وإلى حد الآن يعتبر الوانكينغ (WANKing) أولى أشكال الهاكتيفيزم.[210]

ومثل ما هو الحال في العلاقات الدولية، الهاكتيفيزم يمكن أن يمتد من مبادرة شخص واحد، إلا تحالفات شاملة، مثل ما هو الحال مع أنونيموس، كما أنع معظم الأشخاص الذين يشاركون في هذه العمليات لا يجب أن يكونوا بالضرورة على دراية جيدة بالعلوم الحاسوبية والبرمجة، بل الأغلبية ينطبق عليها ما يسمى بـ (script kiddies)، أي الأشخاص الذين يريدون المشاركة، ويقومون بتحميل برامج

---

[207] Elinor Mills, "Old-time hacktivists: Anonymous, you've crossed the line," in: ***http://goo.gl/scRH13***, (Saturday, 28 May 2016).

[208] 2600, THE CHAOS COMPUTER CLUB, THE CULT OF THE DEADCOW, !HISPAHACK, L0PHT HEAVY INDUSTRIES, PHRACK, PULHAS, "LoU Strike out with International Coalition Of Hackers," in: ***http://goo.gl/iwRRq3***, (Saturday, May 28, 2016).

[209] Loc. Cit.

[210] P.W Singer, Allan Friedman, ***op.cit***, p. 77.

جاهزة من أجل ذلك، ويكون دعمهم عبر النقر فقط، وتعقيد العمليات يمكن أن يمتد من هجوم حجب الخدمات الذي يعد سهلا، إلى عمليات جد معقدة كالتي حصلت سنة 2004، لما قام مجموعة من الهاكتيفيزت بالتسلل إلى شبكة مختبر هانتينغتون (Life Science testing Lab) الذي سُربت أشرطته من قبل والتي فضحت الطرق الغير أخلاقية التي كان يمارسها ضد الحيوانات، الأمر الذي دفع بالهاكتيفيزت إلى تسريب الوثائق ، وأسماء الأشخاص العاملين في المختبر، وعناوين منازلهم، والشراكات القائمة لهذا المختبر، الأمر الذي فضح العديد من المستثمرين الذي ظنوا أن تعاملاتهم ستكون سرية، كما أن الجيران الذي كانوا يقطنون أمام المختمر أزعجهم الأمر وطالبو بتوقف مثل هذه الأشكال من التعذيب المزعوم من اجل العلم، كما تم الاعتداء بالغاز المسيل للدموع على العديد من موظفي الشركة من قبل أشخاص مجهولين، وقد ذهب الأمر حتى إلى سحب الشركة التي يتبع لها المختبر من سوق الأسهم، ولكن في النهاية تم إتهام وإدانة العديد من الهاكتيفيست الذين شاركوا في العملية لأسباب تتعلق بالتحريض عبر الأنترنت، ولكن لا أحد منهم اعلن ندمه على قيامه بذلك.[211]

في سنة 2013 كنت أحد المشاركين في فرق أنونيموس التي كانت تنتمي إلى الجزائر، وذلك في عملية اطلقنا عليها اسم (OpIsrael)، والتي كانت تهدف إلى التأثير على المصالح الإسرائيلية، وتقليل تواجدها في الشبكة العالمية، عبر الهجوم على المواقع الحكومية والتجارية، فقد شارك في العملية أشخاص من مختلف أنحاء العالم، أمريكا الشمالية، والجنوبية أروبا، وآسيا وأستراليا، وإفريقيا؛ الأمر الذي أدى بالعديد من زملائنا إلى المحاكم خاصة في الدول التي لديها نظام قضائي محكم فيما يخص الجرائم الإلكترونية، أو حتى مطالبة إسرائيل من العديد من الدول، عبر توفيرها لبيانات بعض الأشخاص الذين هم يهاجمون فيها. فالهجمات كانت تهدف إلى الوصول إلى الراي العام العالمي فيما يتعلق بقطاع غزة، وانتهاك إسرائيل لحقوق الإنسان، ولم تكن هناك أي نوايا تتعلق بالمصالح المادية، رغم أن الخسائر من الجانب الإسرائيلي تعد مؤكدة خاصة بعد الإعلاق عبر حجب الخدمة للعديد من الوكالات السياحية والبنوك، ومنصات التبادل الإلكتروني، وقد تطلب تنفيذ ذلك في بعض الأحيان استثمار مادي بسيط في الحواسيب التي تقوم بالهجوم.

يجدر الذكر هنا أن أنونيموس لا تعبر على أحد، ولا أحد يمتلك هذا الاسم، فتحالف أنونيموس تكمن هويته في طبيعة العمليات التي يقوم بها، والتي في الغالب تكون لصالح قضايا مهمة وأحداث راهنة، لهذا تكلمت من قبل على الثقافة الجديد التي خلقها المجتمع الإلكتروني، إذ لا يمكن اعتبار الابتزاز من اجل

(211) **Ibid**, pp. 79.

المال كأحد مميزات أنونيموس. عكس ما يمكن القول عن العملية التي شنت ضد موقع بايبال (Paypal) للدفع الإلكتروني والتي تسببت في إغلاق الموقع لمدة 7 أيام وذلك بسبب رفض هذا الأخير دفع التبرعات لموقع ويكيليكس.[212] مثل هذه العمليات لها نمطية واضحة وتجسد ثقافة الهاكتيفيزم وأنونيموس.

هناك من يرى أن الهاكتيفيزم هو نوع من العصيان المدني والنهوض ضد النظام والسلطة القائمة، كما يعبر أيضا على محاربة هيمنة الدولة، والقوة الدولية المختلفة؛ ولكن في الحقيقة، يجب على كل شخص يتعاطى مع مثل هذه المجموعات أن يكون حذر، أو على دراية بما يحدث، فمثلا في الأحداث العربية التي أدت إلى سقوط العديد من القادة، هناك شركات عديدة قدمت الدعم للمتظاهرين مثل ما هو الحال مع غوغل (Google)، وتويتر (Twitter)، وسكايب (Skype)، مثل هذه الأمور والمساهمات تفسد الصورة التي يدعو إليها الهاكتيفيزم، كم أن الدول أصبحت تعمل بطريقة أكبر على إدراج عملاء مزدوجين داخل هذه المجموعات الإلكترونية، الأمر الذي سينعكس على طبيعة العمليات، ومصداقيتها.[213]

في الأخير وبعد دراستنا للعديد من الوسائل التي يمكن استخدامها للكفاح ضد الهيمنة على مختلف مستوياتها، يمكننا أن نرى أن العالم، اصبح أكثر تعقيدا، وأكثر تشابكا في نفس الوقت، الأمر الذي ببروز مثل ذه الظواهر، فالفضاء الإلكتروني هو بمثابة امتداد للحياة في الواقع الذي نعيشه، وهو يعبر على ممارسة هذه الحياة بأساليب أخرى، وربما بطرق أكثر أمامنا في بعض الأحيان، فالتطور الرقمي اسمح للفواعل الغير رسمي باقتسام السيادة مع الدولة، كما سيطرتها أيضا على مختلف شؤون حياة مواطنيها، فالذي ذكرناه هنا مع الإرهاب الإلكتروني، والنشطاء الإلكترونيين، والدولة، والجريمة المنظمة الإلكترونية، هي مجرد عناوين كبيرة لأجزاء صغيرة من ما يشكله الصراع الإلكتروني العالمي، فكون هذا الصراع اصبح يتعلق باقل وحدة ممكنة في العلاقات الدولية، والذي هو الإنسان، يجعل من التكهن بحدود أفعال

---

(212) Brian Njama Kiboi, ***Cybersecurity as an Emerging Threat to Kenya's National Security***, Master's Thesis, not published (University of Pretoria: Department of Political Science, 2015), p. 51.

(213) P.W Singer, Allan Friedman, ***op.cit***, p. 80.

هذا الأخير شيء مستحيل، ويصعب إيجاد الأنساق، والأنماط السائدة، والثابتة، والتي تتميز بنوع من الاستقرار، والثبات.

2.4 الدراسات الحربية

تتمثل الدراسات الحربية (War Studies) في مجمل الدراسات التي لها علاقة بتاريخ الحرب، والدراسات الاجتماعية الحربية، وعلم الحرب، وقانون الحروب، وفلسفة الحروب، والعديد من الدراسات التي لها علاقة بالحرب ، مثل العلاقات الدولية، والاقتصاد، وتحليل النزاعات، ودراسات السلام؛ لكن الذي يهمنا هنا رؤية التطورات التي حدثت لمفهوم الحرب، كما أن الفهم الجيد للصراعات التي تحدث حاليا في العلاقات الدولية، يجب أن يكون وفقا لدراية تامة لكيفية تطور الوسائل الإكراه، ومن أجل فهم أحسن واعمق، لتطور العقيدة العسكرية، وتعدد وتطور مختلف الفواعل التي تحدد ماهية الحرب، إذ أن الحرب كانت تعد ميدان الدولة، فالحرب لها علاقة بالسيادة، ولا يمكن لأي كان أن يعلن الحرب، حتى أنه يمكننا أن نجد العديد من التصنيفات التي لها علاقة بالحروب، إذ أن إطلاق صفة الحرب على حالة معينة، يتطلب عدة شروط لها علاقة بالقيمة العددية للجيش، والضحايا، والخطابات الرسمية، والقانونية، مثل ما هو الحال حاليا مع بروتوكولات جينيف، لهذا سأحاول طرح هذه السلسلة التاريخية لتطور الحرب، ومختلف الأسس النظرية، والاستراتيجيات المختلفة التي كانت تقوم عليها، من اجل رؤية ماذا تمثله الحرب الآن من ما كانت عليه، وما موضع الأمن الإلكتروني من الصراعات الحالية.

2.4.0 الجيل الأول

يمكن النظر إلى أجيال الحروب ابتداء من صلح وستفاليا سنة 1648 (Peace of Westphalia)، فهذا الاتفاق الذي أنهى ثلاثة سنوات من الحروب، أنهى أيضا لامركزية السلطة والقوة، إذ بعد هذا الاتفاق، أصبحت الحرب من اختصاص الدولة ذات السيادة فقط، فقبل هذا الاتفاق، كانت هناك العديد من القبائل والعائلات، والمدن، التي بإمكانها شن الحروب، وذلك عبر استخدام طرق مختلفة،

وليس فقط الجيوش، إذ أن هذه الطرق امتدت من عمليات الاغتيال، إلى الرشاوي، والتجسس والفضح، والابتزاز. [214]

يمكن النظر إلى الحروب من الجيل الأول، على أنها تلك الحروب التي استخدمت تكتيكات الهجوم الخطي، هذه التكتيكات، ومثل بقية الحروب، تكون قد طُورت جوابيا للتكنولوجيات التي كانت سائدة، فالهجوم الخطي، كان يوفر طاقة قتالية اكبر، كما كانت توفر طاقة نارية أكبر أيضا، بالإضافة إلى هذا تتميز هذه الحروب على أنها تتطلب جهود كبيرة خاصة فيما يتعلق بوتيرة الإطلاق الناري، فالجيل الأول كان يتعامل مع الحروب بطريقة بدائية نوعا ما، وهي لا تختلف كثير عن الحروب القديمة عند الرومان والمسلمين إلا من ناحية التكنولوجية المتقدمة، والتنظيم الشبه قانوني للجيش، كما أن الاستراتيجيات الخطية التي كانت تُعتمد لم تتطلب تدريب عالي للجنود، بالإضافة إلى هذا فإن عدد الضحايا كان كبيرا مقارنة بمتوسط تعداد الجيش.[215]

لقد امتد هذا الشكل من الحروب من سنة 1648 إلى سنة 1860، وفي هذه الفترة تجسدت العديد من الأفكار التي لا زالت تعد موجودة حاليا في الجيوش، مثل ما هو الحال مع التكوين العسكري لبعض القادة، واللباس الرسمي، وطريقة التحية، رغم أن العديد من الأشكال التي عرضناها هنا كانت موجودة مسبقا، إلا أن هذه الفترة كانت لها تأثير كبير في طريقة تنظيم الجيوش التي نراها اليوم، خاصة في ما يتعلق بالنظام الداخلي، والعقيدة العسكرية للقوات البرية، والانضباط، وطرق التدريب؛ أما فيما يخص الاستراتيجيات الخطية التي تكلمنا عنها، فقد بدأ تراجعها الكبير في أواسط القرن 19، والذي كان نتيجة تطورات تكنولوجية جديدة، جعلت من الإستراتيجية الخطية والانضباط الخطي في ساحة الحرب لا معنى له وغير مفيد ويمكن اعتباره بمثابة انتحار فعلي، خاصة من بداية ظهور الأسلحة الرشاشة (Machine Gun).[216]

كل هذه المعطيات، وبالأخص تلك التي لها علاقة بالتطور التكنولوجي، والاكتشافات العلمية، جعلت من الجيل الأول للحروب غير عملي من عدة نواحي، رغم أن هذا الشكل كان موجود في العديد

---

[214] William S. Lind, "Understanding Fourth Generation War," in ***MILITARY REVIEW***, (September - October, 2004), pp, 12-16.

[215] William S Lind, Keith Nightengale, John F Schmitt, Joseph W Sutton, Gary I Wilso, "The Changing Face of War: Into the Fourth Generation**,**" in Marine Corps Gazette (pre-1994), No 10, Volume 73(October, 1989), pp. 22-26.

[216] William S. Lind, ***op.cit*, "Understanding Fourth Generation War".**

من المناطق التي لم تتوفر على قدرة صناعية أو تقنية، إلا أن المقاييس كانت قد تغيرت إلى ما يسمى بالجيل الثاني للحروب.

2.4.1 الجيل الثاني

لقد برز الجيل الثاني من الحروب، بعد التناقض الكبير الذي حضل في الثقافة التقليدية للاستراتيجية الخطية التي تستند إلى الانضباط، والمعطيات التي تتعلق بالجغرافيا، إذ أن السلوك التقليدي للحروب الذي كان موجود في الجيل الأول، لم يصبح موجود حاليا بشكل كبير، خاصة وأن متغيرات الحرب قد تغيرات، كما أن التقانة في حد ذاتها فرضت مجموعة من التغيرات، فالطريقة الخطة للجيل الأول، والتي تم تجسيدها في الحرب العالمية الأولى من قبل القوات الفرنسية، وذاك بدفع الهجوم الخطي من الخنادق، الأمر الذي كان مميت بدرجة كبيرة بسبب توفر الرشاشات.

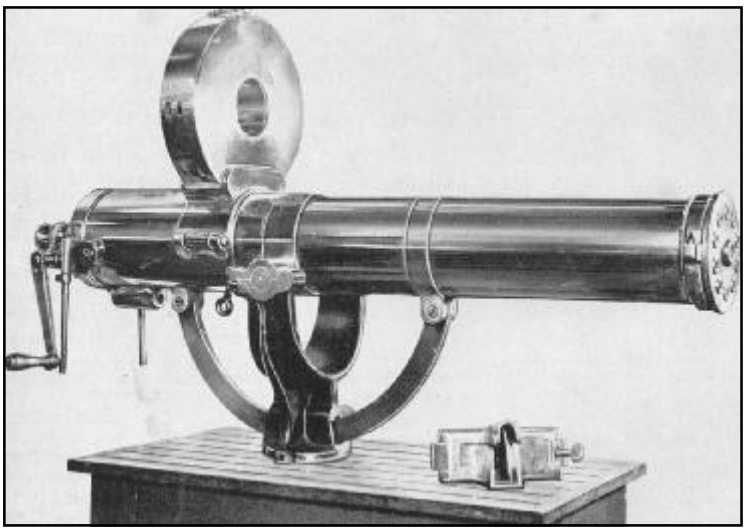
لقد قلنا من قبل أن الجيل الأولى، والنهج الأول في الحرب بدأت تقل أهميته بشكل كبير بداية أواسط القرن 18، وقد طرحنا أن ذلك بسبب توفر تكنولوجية جديدة جسدت في الأسلحة الرشاشة، ويمكننا فهم ذلك عبر قيام المخترع الأمريكي ريتشارد غاتلين (Richard Jordan Gatling 1818-1903) باختراع، وإنتاج سلاح الرشاش الذي أطرق عليه اسمه (Gatling)، وتعد الغاتلين أول سلاح رشاش ناري ناجح،[217] ويمكننا أن نرى في **الصورة رقم 2.1** أحد النماذج الأولية لهذا السلاح، فقد هدف غاتلين إلى التقليل من تعداد الجيش أثناء الحروب، لكن الذي قام به في الحقيقة، هو تغيير في طبيعة الحرب في حد ذاتها مثل ما فعلت القنابل النووية، ومن هنا يمكننا أن نفهم، أن الهجوم الخطي لا فائدة منه، وقد كانت النتائج أثناء الحرب العالمية الأولى خير دليل على ذلك.

بالإضافة إلى هذا، فالجيل الثاني من الحروب تميز باعتماده على المدفعية (Artillery)، وذلك وفق عقيدة المدفعية تغزو والمشاة تحتل، ولهذا نجد بروز تخطيط مكاني من أجل التنسيق بين المدفعية والقوات البرية، والمدرعات، والتي كان

[217] Horach Greeley, Leon Case, Edward Howland, John B. Gough, Philip Ripley, F. B. Perkins, J. B. Lyman, Albert Brisbane, Rey. E. E. Hall, and others, **The Great Industries of The Unites States** (The United States of America: published by Hartford, 1872), pp. 944-950.

القائد في هذه المهمة هو بمثابة مسير لأوركسترا (Orchestra) واسعة النطاق. هذا النموذج من الحروب لا زال موجود حتى حاليا، فرغم أن الولايات المتحدة الأمريكية تخلت على هذا النوع من الحروب، كطريقة أساسية للحرب بعد 1980. [218]

الصورة رقم: 2.1



أحد النماذج الأولى للغاتلين، بـ 10 مواسير إطلاق. [219]

إلا أنه يمكننا رؤية بعض مؤشرات الجيل الثاني، في حرب أفغانستان والعراق، والتي يقول المحللون أنها تميزت بالطريقة الأمريكية لشن الحروب أثناء الحرب العالمية الثانية، والتي تسمى بـ رمي الحديد على الهدف (Putting steel on target)،[220] ونفس الأمر يتعلق بدور القوات الجوية والبحرية، اللذان أخذا حصة اكبر من متوسط حجم القوة النارية المستعملة في الجيل الثاني من الحروب، فالجيل الثاني من الحروب يعبر على النهضة الصناعية بطريقة واضحة جدا.

---

[218] William S Lind, Keith Nightengale, John F Schmitt, Joseph W Sutton, Gary I Wilso, ***op,cit.***

[219] Larry Jewell, Patrick Clancey, HyperWar Foundatio, "MANUALLY OPERATED MACHINE GUNS," in: ***https://goo.gl/4xTB51***, (Monday, May 16, 2016).

[220] William S. Lind, ***op,cit.***

- **المشميكا:** وتعبر عن المشاة الميكانيكية، استراتيجية البليتزكريغ تعتمد بشكل كبير على المدرعات في طريقة عملها، ودخول المدافع، والمدرعات، والمشات الميكانيكية، يكون مباشرة بعد انتهاء القصف البساطي.
- **القصف البساطي:** عبارة عن رمي قنابل تنفجر عن الاتصال بالأرض، استعملت كثيرا في الحربين، لا تمتاز بالدقة، لكنها ساهمت في تدمير العديد من الدول الأوروبية بنسبة فاقت 97%.

2.4.2 الجيل الثالث

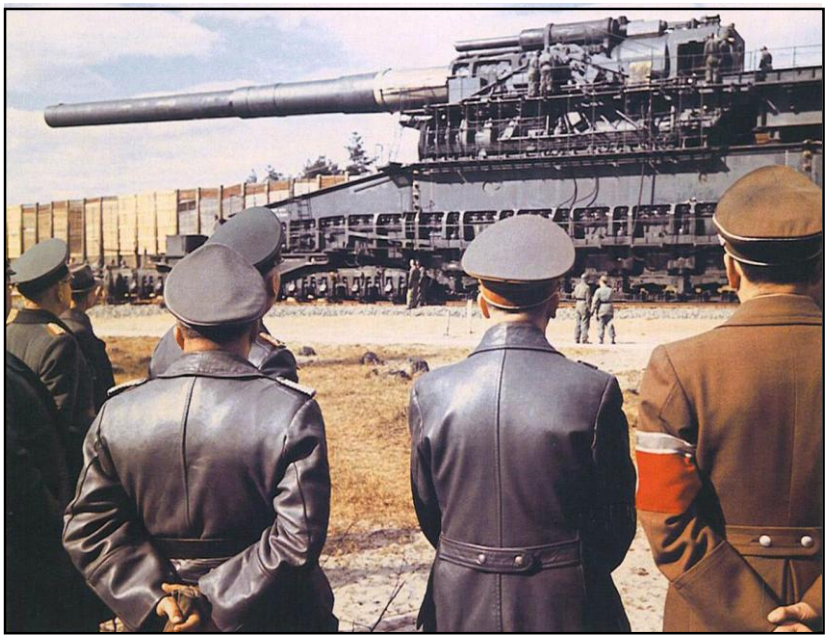
ينظر إلى الجيل الثالث من الحروب على أنه الجيل الوحيد الذي لا يستند إلى قاعدة تكنولوجية من أجل تحديده، وذلك أن هذا التحول، أو بروز هذا النوع الجديد، يستند إلى مجموعة من الاستراتيجيات التي لها علاقة بطريقة تسيير الحرب، وطريقة تقدير المحيط واستخدام المعطى المكاني والتكنولوجي من أجل تحقيق الأهداف، وهذا ما أكده المنظر الأمريكي في قضايا البحث والدفاع **روبرت بانكار** (Robert J. Bunker) حين تكلم على بروز ما يسمى بـ الحرب الخاطفة، أو البليتزكريغ (Blitzkrieg)؛ وتمثل هذه الإستراتيجية تغيرا فعليا في طريقة ممارسة الحرب، إذ أصبحت تعتمد على السرعة، فقد استخدمت هذه الإستراتيجية لأول مرة من قبل الألمان في الحرب العالمية الثانية، والتي كانت تهدف إلى احتلال أماكن واسعة جدا في اقل وقت ممكن، وذلك عبر القيام أولا بقصف بساطي من قبل طائرات قاذفة، ثم يلي الأمر قصف متواصل من قبل مدافع طويلة المدى، يليها احتلال مباشرة من قبل المدرعات، ثم تأتي ورائها المشميكا(المشاة الميكانيكية) في عملية منسقة بطريقة عالية جدا وسريعة أيضا، فهذا النوع من الحروب كان يركز أكثر على عامل الوقت، من العامل المكاني.[221] الأمر الذي يمكننا أن نفهمه في سعى ألمانيا على امتلاك يا يسمى بالمدافع الفائقة المدى (Super Cannon) على غرار اكبر مدفع من حيث العيار (800 ملم) والحجم إلى حد الآن، وهو المدفع الثقيل غوستاف (Schwerer Gustav) الذي أعتبر أحد إفرازات هذه العقيدة الجديدة في ممارسة الحرب، والذي يمكن رؤيته في **الصورة رقم 2.2.**

بالإضافة إلى هذا نجد أن الجيل الثالث من الحروب، أعطى أهمية اكبر، ودورا اكبر للضباط السامين، وضباط الصف، ولهذا نجد بروز مصطلح ألماني يشير . التكتيك الهجومي النوعي (Auftragstaktik - Mission-type tactics)، والذي يشير إلى إعطاء القائد للضباط المهمة، والهدف، والقوات، والزمن المحدد، لكن للضابط حرية أكبر في طريقة تحقيق الأهداف التي أمر بها من الناحية العملياتية؛ لهذا يقوم القادة بإعطاء أوامر واضحة ودقيقة وشاملة، وللضباط ليونة أكثر في التعامل، الأمر الذي سيوفر الوقت، كما سيعطي للضباط ديناميكية عمل وتجربة أكثر في حال انقطاع الاتصال.[222]

الصورة رقم: 2.2

---

[221] ROBERT J. BUNKER, "Generations, Waves, and Epochs MODES OF WARFARE AND THE RPMA," in **AIRPOWER JOURNAL**, No 1, Volume X(1996), pp. 1-10.
[222] William S. Lind, ***op,cit.***



أدولف هتلر –الثاني بعد اليمين– (Adolf Hitler 1889-NA)

في دورة تفقدية لمدفع غوستاف سنة 1941.[223]

يمكننا أن نرى هنا أن المبادرة أصبحت أكثر أهمية من إتباع الأوامر، ونحن نتكلم خاصة على المبادرات التي تأتي بنتائج جيدة، وذلك في ظل البحث المستمر على السرقة في تحقيق النتائج على الأرض. فالجيل الثالث من الحروب، ومثله مثل باقي النماذج أو الأجيال، يعد نموذجا قائما ومستمرا إلى حد الآن، فالأجيال التي تعبر على فناء جيل واستمرار الجيل التالي، بل هي تعبر على بروز أشكال جديدة، وسنرى أن القادة العسكريين عملوا في العديد من العمليات القتالية على استخدام استراتيجيات مختلفة تخدم الهدف النهائي، الأمر الذي يدفع بنا إلى التفكير بأن الأوضاع المكانية، هي التي تفرض في بعض الأحيان نوع الإستراتيجية المتبعة.

[223] RHP, "The Heavy Gustav, Hitler and generals inspecting the largest caliber rifled weapon ever used in combat, 1941," in: ***http://goo.gl/Wd0Cy6***, (Monday, May 16, 2016).

2.4.3 الجيل الرابع

يمثل الجيل الرابع من الحروب، نقلة نوعية في الإستراتيجية العسكرية، والتكنولوجية المعتمدة أيضا، إذ يمكننا أن نرى اختلاف فعلي للعقيدة العسكرية على الأجيال السابقة رغم عدم زوالها، ففي ميدان الحروب، نحن نتكلم أكثر على بروز تحديات، وسائل موازية للممارسة الحرب، أو محاكات الاستراتيجيات التقليدية، عبر استخدام تقنيات حديثة ومعاصرة، فالجيل الرابع من الحروب، أو الفترة التي برز فيها هذا الجيل، برزت فيها العديد من أشكال الحروب التي يمكنها أن تعطينا فكرة على محددات هذا الجيل.

فهذا الجيل يشتمل على مجموعة واسعة من أشكال الحروب مثل الاستباقية أو الوقائية (Preventive War)، والحروب اللامتماثلة أو الغير متماثلة (Asymmetric Warfare)، كما بروز أيضا ما يسمى بحروب مكافحة التمرد التي مُورست ضد المستعمرات الأوروبية السابقة مثل الجزائر (Counter-Insurgency War)،[224] وبروز نوع مميز من الحرب أيضا تسمى بالحرب القانونية (Lawfare) فالحرب القانونية كمصطلح برز لأول مرة في قاموس أكسفورد (Oxford English Dictionary) سنة 2001 ، وأنتشر استعماله خاصة بعد أن أستعمله الجنرال الأمريكي **شارلز دانلاب** (General Charles Dunlap) في محاضرة في جامعة هارفارد حيث عرف الحرب القانونية على أنها:[225]

> "**الإستراتيجية التي تقوم على الاستعمال الصائب، أو الغير صائب للقانون بالإضافة إلى الوسائل العسكرية التقليدية، وذلك من أجل تحقيق الأهداف المرجوة**".

بالإضافة إلى هذا، يمكن إضافة النموذج اللامركزي للحروب والتنظيم القتالي(Decentralized organizational) ، كما أخذت الحروب بالوكالة أهمية اكبر خاصة أثناء الحرب الباردة (Proxy War

---

[224] Thomas X. Hammes, "Insurgency: Modern Warfare Evolves into a Fourth Generation," in **The Strategic Forum**, No 214(January, 2005), pp. 1-8.

[225] Michael Scharf, Elizabeth Andersen, Effy Folberg, Michael Jacobson, Katlyn Kraus, "IS LAWFARE WORTH DEFINING?," in **Case Western Reserve Journal of International Law**, No 11, Volume - Case 43(Sepetember, 2010), pp. 11-27.

) خاصة من قبل الدول الكبرى، [226]فالجيل الرابع للحروب، لازال في تطور لحد الآن، ولكن هناك من يضيف الجيل الخامس الذي سنناقشه لاحقا.

يمكننا أن نجد في الجيل الرابع من الحروب، تقنيات استمر تحديثها عبر التاريخ إلى حد الآن، فقد تكلمنا من قبل على رشاش غاتلين الذي يعد أهم مميزات الجيل الثاني من الحروب، ولكن رغم هذا يمكننا إيجاد نفس التصاميم المحسنة حاليا، بل سنجدها حتى على بعض العتاد والأسلحة الأيقونية الموجودة في القوات العسكرية الحالية، وأفضل مثالا على ذلك هو اعتماد طائرة الدعم والإسناد الجوي القصير المدى (Fairchild A-10 Thunderbolt II)، على نموذج سليل النموذج الأولي الذي ذكرناه من قبل والذي

الصورة رقم: 2.3

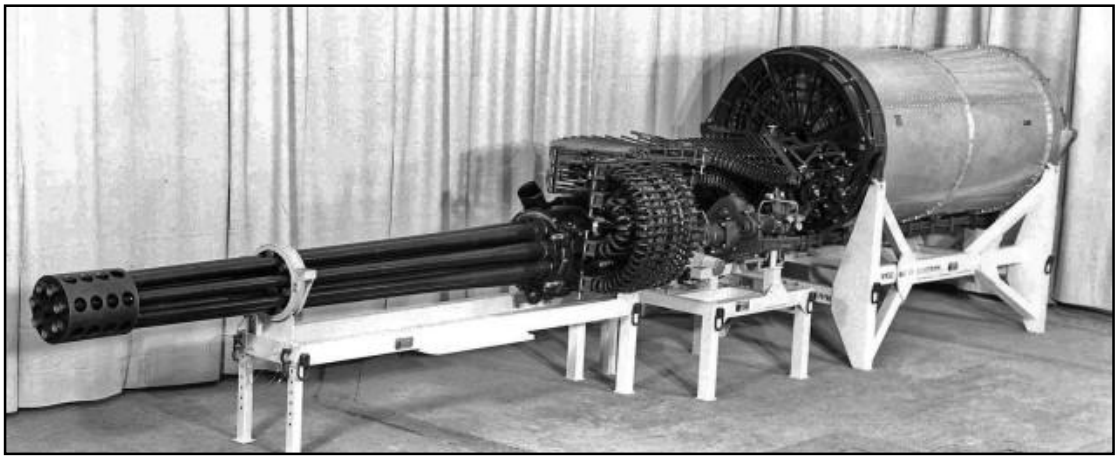
صرب من طائرات فيرشيلد أي–10 في تشكيلة الأصابع الأربعة (Finger-Four). [227]

يتعلق بـ الغاتلين، ويمكننا أن نرى في **الصورة رقم 2.3**، النموذج المستعمل حاليا في طائرة فيرشيلد. ما يهمنا هنا، هو أن نفهم، ونعرف أن وجود أجيال جديدة لا يعني بالضرورة انتقال راديكالي في التكنولوجية، أو العقيدة العسكرية، أو الاستراتيجيات المعتمدة، بل يمكن أن تكون بمثابة تحديث لهذه الاستراتيجيات، ويمكننا أن نرى هذا الطرح حاليا فيما أصبح يُطلق عليه بالحروب *الهجينة (Hybrid warfare

[226] Nick Turse, ***The changing Face Of Empire: Special Ops, Drones, Spies, Proxy Fighter, Secret Bases, And Cyber Warfare*** (The Unites States of America: Chicago, published by Haymarket Books, the first edition, 2012.), pp. 188-222.
[227] Becky Vanshur, "KC-135s refuel Idaho's A-10s in mid-flight," in: ***http://goo.gl/plEVoD***, (Tuesday, May 17, 2016).

)، [228] بل هناك حتى من يشير إلى أن بعض الاستراتيجيات التي استخدمت أثناء الجيل الأول من الحروب، تعبر في مضمونها على نظرة الجيل الرابع في الحروب، ويمكن رؤية ذلك في حصار تركيا لفيينا سنة 1683 حيث أن المسلمين طورا ما يسمى بالاحتلال عبر الاستيطان (invasion by immigration) الذي لا يقل خطورة عن الاحتلال العادي.[229]

الصورة رقم: 2.4



رشاش غاتلين من نوع(GAU-8/A Avenger)؛ الرشاش الأساسي لطائرة فيرشيلد.[230]

إلى جانب أشكال الحروب التي وجدت في الجيل الرابع من الحروب، فالجيل الرابع من الحروب أيضا تميز بأفكار جديدة تجسدت في حرب الأفكار، والمشاعر؛ فالدولة لم تعد تسيطر على حدودها بشكل كامل، هذا إلى جانب بروز فواعل غير رسمية في العلاقات الدولية، لهذا يمكننا أن نقول أن الجيل الرابع من الحروب تميز ببروز أفكار جديدة، واستراتيجيات جديدة، وتكنولوجيات جديدة إلى جانب التي كانت موجودة،[231] لكن الشيء المميز هنا أن معظم الباحثين الذي عالجوا قضية الجيل الرابع من الحروب، لم يتطرقوا إلى الأمن الإلكتروني، أو الحرب الإلكترونية كمحدد أساسي لهذا الجيل رغم أنهم

---

[228] Frank G. Hoffman, "Hybrid Warfare and Challenges," in **National Defense University Press**, Volume – Issue 52(1st quarter, 2009), pp. 34-39.

- الحرب الهجينة (Hybrid warfare): نوع من الحروب، يشتمل على استراتيجيات من عدة أجيال في نفس الوقت، من استراتيجية الصدمة والرعب، إلى الحرب الإلكترونية، إلى الحرب الفضائية، إلى البليتزكريغ؛ كما تتميز باستخدام أسلحة وعتاد من أجيال مختلفة أيضا.

[229]William S. Lind, ***op,cit.***

[230] Juerg Studer, ***Are There Five Rings or a Loop in Fourth Generation Warfare? A Study on the Application of Warden's or Boyd's Theories in 4GW*** (The Unites States of America: Alabama, published by BiblioScholar, 2012), pp.7-11

أشاروا إليها، الأمر الذي دفع بالعديد من الباحثين إلى محاولة التطرق إلى الجيل الخامس من الحروب، الذي يعد بمثابة قفزة جديدة في التفكير، والتقانة، والاستراتيجية.

2.4.4 الجيل الخامس

الجيل الخامس من الحروب هو الجيل الذي له علاقة بالتكنولوجيات المتقدمة، والحرب الإلكترونية، والافتراضية، والمعلوماتية، وكل ما له علاقة بالمعلومات، والتقانة، فقط طرحنا هذا التسلسل التاريخ في من أجيال الحروب، كي نستطيع أن نفهم كيف يمكن للتقانة الجديدة أن تؤثر على المعادلة في الصراع الدولي، وكيف يمكن أن تؤثر الأفكار أيضا في تحديد قواعد اللعبة في السباق نحو الهيمنة العالمية، لقد تمكنا من رؤية أن الجيل الرابع من الحروب تميز ببروز فواعل غير رسمية في العلاقات الدولية، رغم أن وسائل الإكراه التي تم اعتمادها تقليدية إلى حد ما، أما الآن ومثل ما حدث مع الغاتلين، برز صراع جديد في العالم يستند إلى قواعد البيانات والقدرة التكنولوجية والأمن الإلكتروني، فالهيمنة العالمية يمكن اعتبارها كامتداد طبيعي للسطلة والهيمنة في الساحة الدولية، وبدا جد واضح أن الأمن الإلكتروني، يعد كأحد الأسلحة التي يجب السيطرة عليها من أجل الخوض في هذه الحرب، من اجل الدفاع على مصالح الدولة، أو الهجوم على دول أخرى، أو حتى قيام أشخاص، أو منظمات، أو جهات مجهولة، بالعمل على إطاحة، أو التأثير، على مصالح دولة أو جهات أخرى لأي سبب كان.

إن توالي أجيال الحروب يعد ظاهرة دورية(Cyclical Phenomenon)، وقد أصبح حقيقة لا يمكن إنكارها خاصة وأن الكثير من الباحثين يميلون إلى نسيان الأمر بعدم تركيزهم على أجيال مستقبلية محتملة،[232] فالجيل الخامس من الحروب لا يمكن تحديده بدقة بسبب أن المعطيات الكاملة لا يمكن معرفتها بشكل جيد، لكن الواضح هنا، هو بروز ميادين جديد للحرب والتي لها علاقة وطيدة بالأمن الإلكتروني، والسعي على الهيمنة الدولية، والتي في الغالب تكون إما عبر هيمنة اقتصادية، أو عسكرية؛ فبعض النظر عن هذه الميادين مثل ما هو الحال مع الحرب الفضائية (Space warfare)،[233] فهي احد اهم العناصر في الجيل الرابع، والجيل الخامس، فمثلا لا يمكن لدولة استخدام الأسلحة المجنحة أو

---

[232] Terry Terrif, Aaron Karp, Regina Karp, **Global Insurgency and the Future of Armored Conflict**, (The Unites States of America, Ney York, published by Routledge, the first edition, 2008.), pp. 9-8.

[233] Jack Hitt, "The next battlefield may be in Outer Space," in: **http://goo.gl/lJ7kVG**, (Wednesday, May 18, 2016).

الجوالة(Cruise Missiles)، بدون نظام فعال للأقمار الصناعية رغم وجود تكنولوجيات تعتمد على الصور ولكنها تعد غير دقيقة في إصابة الهدف، حتى أن الولايات المتحدة الأمريكية يعرف على أنها تعتمد بطريقة كبيرة على الاتصالات الفضائية أثناء العمليات القتالية، ويبدو أن الصين فهمت هذا جيدا، وقامت بإرسال رسالة للعالم عبر قيامها بإسقاط قمر صناعي للأحوال الجوية (FY-1C) الخاص بها باستخدام نظام صاروخي مضاد للأقمار الصناعية (Anti-Satellite Weapon - ASAT) سنة 2007،[234] فالحرب في توسع كلما مر الوقت، من ميدان البر والبحر، إلى الهواء، إلى الفضاء الخارجي، إلى الفضاء الإلكتروني، والمهم هنا، أن الميدان الأخير المذكور، يتحكم في معظم آليات عمل الميادين التي قبله.

بالإضافة إلى هذا، فحروب الجيل الخامس، لا يمكن معرفة إن كانت موجودة أو لا بحكم طبيعة عملها، إذ عكس الأجيال الأولى، فهي غير مرئية، وكما وضحنا سابقا، فالجيل الخامس سيتميز بالدور الذي ستلعبه الفواعل الغير رسمية في رسم صورة الصراع الذي يحدث في العلاقات الدولية، فتراجع مركزية الدولة، جعلت دورا أكبر للفرد في اللعب مع العمالقة، فالطرح التي يتكلم عليه الأمن الإلكتروني، هو تلك العمليات التي تهدف إلى مكافحة امتداد نفوذ أي جهة معينة، أو حتى أفكار، أو مناسبات معينة، ويمكن أن تطال العمليات حتى الأقمار الصناعية عبر قرصنتها(Satellite Disruption)، ولكن في الحقيقة، فإن الجيل الخامس الذي يضع في مقدمته، دور الفواعل الغير رسمية، وبروز الأسلحة الإلكترونية المتقدمة، لا يمكن التكهن به، ومعرفته جيدا في ظل اللامركزية الكبيرة جدا والخطيرة في نفس الوقت، وهذا ما أكده القائد العسكري الأمريكي **شانون بيب** (Shannon Beebe)،[235] حيث قال أن حروب الجيل الخامس لن تَعرض أو تَصف جيوش معينة أو أفكار محددة بل ستكون:[236]

"دوامة من العنف(Vortex of violence)، أين ستكون للجميع الحرية في ممارسة التدمير".

وهذا ما يعبر عليه مفهوم الأمن الجديد تماما، ففي ظل الهيمنة، ورقمنة معظم أشكال الحياة الإنسانية، وبروز فواعل غير رسمية يمكن حتى أن تحدد كشخص، أي حرب، أو صارع سيكون بمثابة

---

(234) Jaganath Sankaran, "China's Deceptively Weak Anti-Satellite Capabilities," in: ***http://goo.gl/VP3Bas***, (Wednesday, May 18, 2016).

(235) J.R. Wilson, "Cyber warfare ushers in 5th dimension of human conflict," in: ***http://goo.gl/VpBVDu***, (Wednesday, May 18, 2016).

(236) David Axe, "How to Win a 'Fifth-Generation' War," in: ***https://goo.gl/7lmMlq***, (Wednesday, May 18, 2016).

دوامة عنف، أي أن أي شخص يمكنه أن يلحق الضرر بالطريقة التي يريدها، أو يَقدر عليها، فطبيعة العالم الذي نعيش فيه اليوم، جعل الصراع العالمي أكثر دقة، وسرية، ويميل أكثر إلى ثقافة قنص الرؤوس، وتحقيق الأهداف جراحية بأقل أضرار ممكنة، بسبب وجود عالم أصبح الاعتماد المتبادل فيه أحد أهم محدداته، وعلى هذا الأساس، يمكننا أن نلخص معظم المعلومات التي تعاطينا معها في أجيال الحروب في **الجدول رقم 2.0** الذي يوضح مختلف التحولات التي حدثت في ميدان الحروب والصراع الدولي.

الجدول رقم: 2.0

	الجيل الأول	الجيل الثاني	الجيل الثالث	الجيل الرابع	الجيل الخامس
الفترة	1648- 1860	ح.ع.1 وح.ع.2	ح.ع.2 والحرب الباردة	1990- حاليا	حاليا- مستقبل
الأفكار	تأسيس النموذج الأول	تغير تقني	تغير في الأفكار	تغير تقني، فكري	تغير تقني، فكري
الإستراتيجية	الهجوم الخطي	استنزاف	بليتزكريغ	عمليات إرهابية وتدخلات جراحية	مفتوحة، ومتعددة
التقانة	بنادق، حرابة	بنادق رشاشة	المدرعات الميكانيكية	أسلحة ذاتية الصنع	أي نظام قائم على قاعدة رقمية، أو يستند عليها
الفواعل الرئيسية	الدولة الأمة	الدولة الأمة	الدولة الأمة	فواعل غير رسمية	دوامة تفاعلات
الحرب هجينة					

جدول يلخص أجيال الحروب المذكورة في الدراسات الحربية. (إعداد الطالب)

يمكننا في الأخير القول أن هذه النماذج لا تعد نهائية، إذ هناك العديد من الباحثين الذي لهم أراء مختلفة في تقدير الأسباب، والمحددات الدقيقة لهذه الأجيال، ولهذا يمكننا أن نرى أن حدود الفصل ضبابية وغير واضحة خاصة فيما يتعلق بقضية الاعتراف، إذ يقول **ماكس مانوارينج** (Max G. Manwaring

) أنه لو أخذنا بالجيل الرابع للحروب، فإن الولايات المتحدة الأمريكية في حرب حاليا، [237] فالحرب كسلوك اجتماعي، لديه أيضا إفرازات قانونية على المستوى الداخلي والخارجي، فهناك فرق كبير بين وقت الحرب، والسلم، واعتراف دولة ما، بأسلوب حرب معين، يمكن أن يؤدي بها إلى التعامل مع إشكال ضبط الميزانية ، وتبرير النفقات، وهذا ما يعالجه من هم ضد ما يسمى بالجيل الرابع للحروب الذي يرون في ذلك تبريرا غير منطقي للسياسات المالية للإنفاق العسكري، أما إذ مررنا إلى الجيل الخامس، فمن الواضح جدا أن الأمر بمثابة دوامة عنف كما قال **ماكس**، إذ أن مختلف المعطيات المتعلقة بالفواعل الغير الرسمية، والتنظير في العلاقات الدولية، والنظام الاقتصادي، والذكاء الصناعي، تشير إلى الطابع الجديد للصراعات المستقبلية، ومدى التخبط الكبير في البحث على الهيمنة، ومكافحة الهيمنة في نفس الوقت؛ فمعالجتنا لتطور أجيل الحروب، أعطانا فكرة حول مدى تأثير الأفكار، وخاصة التقانة، على الاستراتيجيات المعتمدة في الصراع الدولي، فالإمكانيات في مجال الصراع هي التي تحدد في الأغلب الطريقة التي تعتمد من اجل محاولة التأثير على الجهة الثانية، وبداية انفلات سيطرة الدولة على حدودها، كما تراجع احتكار القوة، ساهم بشكل كبير في بروز أنواع جديدة من الحروب، والصراعات.

2.5 السبرانية

إن النظر إلى السبرانية والتحولات العديدة التي طرأت عليها، يوضح لنا فعلا أن هذا العلم في تطور مستمر، وهو يعتمد مع مرور الوقت على مركبات جديدة تتعلق بالميكانيكا والتحكم، والتواصل، فإذ نظرنا الآن إلى الدراسات السبرانية وقمنا بمقارنتها، بالشكل التقليدي للدراسات السبرانية يمكننا أن نرى اختلافا كبيرا إذا لم نقل جوهريا في هذا النوع من الدراسات.

إن التعاطي من السبرانية، في ظل الدراسة الحالية له علاقة خاصة بطبيعة الموضوع في حد ذاته، إذ أن له علاقة معالجة مختلف التفاعلات، والارتدادات النظرية للأمن الإلكتروني، والقضايا التي تتعلق بالهيمنة في العلاقات الدولية، فمن أجل فهم أعمق للموضوع، يجب التعاطي مع مختلف المعلومات التي يمكن أن تكون لها علاقة مباشرة أو غير مباشرة بالموضوع، وذلك عبر دراسة الأمن الإلكتروني، من

[237] Max G. Manwaring, ***The Strategic Logic of Contemporary Security Dilemma***(The United States of America: published by CreateSpace - U.S Army War College of Carlisle, 2012.), pp. x-11.

منطلق تطبيقي علمي، ومجتمعاتي في نفس الوقت، وسأحاول شرح هذه العلاقة والطريقة في التعاطي، والربط لما هو علمي دقيق بما هو اجتماعي عبر توضيح مدى تأثير كل واحد على الآخر.

"فالتخصصات العديدة التي أصبحت تدرس حاليا تحت حقل السبرانية، جعل من المفاهيم المقدمة لهذا النوع من الدراسات عديدة ومختلفة، في الولايات المتحدة الأمريكية، أو أروبا أو الاتحاد السوفييتي ولهذا صرح شالنج باوكرز (challenge Bowkers) أن هذا التخصص أو هذا المجال الدراسي هو مجال عالمي".[238]

يعد **نوربيرت واينر** (Norbert Wiener 1894 -1964) الأب المؤسس للسبرانية أو السيبرنيطيقية، وقد عبر على ذلك في كتابه السبرانية: أو التحكم والاتصالات في الكائن الحي والآلة، حيث أعلن عن ولادة علم جديد وهو السبرانية، والسبرانية مصطلح مستوحى من الكلمة الإغريقية كيبرنيتيس (Kubernetes) والتي كانت تعني الشخص الذي يقود السفينة، أو القائد (Steersman). أدخل بعد ذلك مفهوم السبرانية على العديد من المجالات العلمية مثل ما هو الحال مع الرياضيات، والهندسة، وعلم دراسة الأعضاء (Physiology)، فقد قام **واينر** بالعديد من الدراسات المتداخلة في مجل أنظمة الاتصال وصناعة الحواسيب، ودراسات تتعلق بنمذجة الجهاز العصبي رياضيا، إلى جانب أبحاث فيما يسمى بالدراسات الترقيعية (Prosthesis). [239]

الأمر الذي يمكن ملاحظته في السبرانية، هو أنه هناك تداخل كبير في التخصصات حتى منذ البداية، ففي طرحه للبداية الأولى لفكرة السبرانية، فقد صرح **واينر** أن البداية كانت خاصة لما كان يعمل مع **جوليان بيغلاو** (Julian Bigelow 1913 - 2003) في مشروع أثناء الحرب العالمية الثانية يتعلق بمضادات جوية، فلاحظ بعد أن ناقش **آرثر رازنبلوث** (Arturo Rosenblueth 1900 - 1970) أن نظريات الهندسة والتحكم والاتصالات يمكنها أن تفسر السلوك أو طريقة التفاعل لكل من الآلات والبشر. هذا الاستنتاج تم التعبير عنه في مقال عنوانه "الهدف والسلوك والغاية"، والذي تم إعداده من

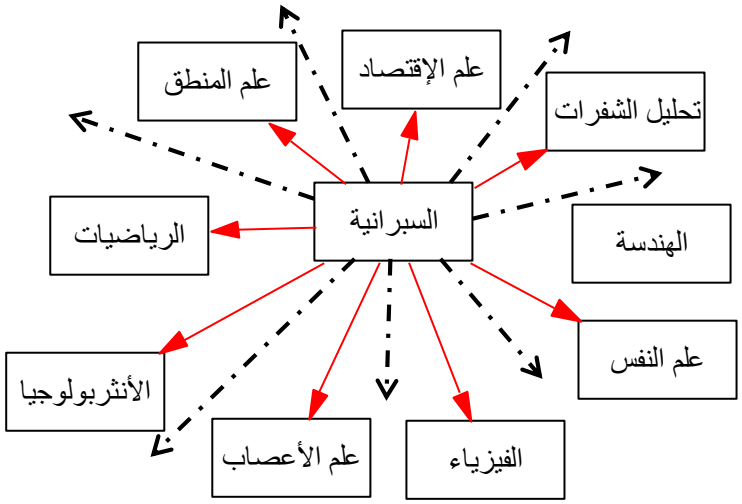
---

[238] David A, Mindell. Jérôme, Segal. Slava, Gerovitch, **Communications Engineering to Communications Science , Cybernetics and Information Theory in the United States, France, and the Soviet Union, in Science and Ideology: A Comparative History**(United Kingdom: London, published by Routledge , the first edition, 2003), pp 66–96.

[239] Ronald, R. Kline, ***The Cybernetics Moment, Or Why We Call Our Age The Information Age*** (The United States of America: Maryland, John Hopkins University Press, the first edition, 2015), p. 11.

طرف **نوربيرت واينر**، و**آرثر رازنبلوث** (Rosenblueth،Arturo)، و**جوليان بيغلاو** (Julian Bigelow 1913 - 2003) والذي أصبح فيما بعد مرجعية مهمة من أجل فهم السبرانية.[240] وتأكيدا مدى اتساع رقعة التخصصات التي كانت مهتمة بالسبرانية يمكننا الاطلاع على سلسلة مؤتمرات مايسي (Macy conferences) والتي امتدت من سنة 1946 إلى سنة 1953 برعاية مؤسسة مايسي التي كانت تنشط في أبحاث الصحة والتعليم.[241] شارك في هذه المؤتمرات العديد من العلماء من عدة تخصصات ويمكن توضيح البعض منها في الشكل التالي:

الشكل رقم: 2.0



شكل يوضح بعض التخصصات للعلماء، والباحثين، الذي

شاركوا في مؤتمرات مايسي، المتعلقة بموضوع السبرانية. (إعداد الطالب)

ولكي نحاول فهم كيف أصبح لعلماء الاجتماع دور في مثل هذه الاجتماعات، فقد تم طرح العديد من التساؤلات من التساؤلات المتعلقة بجدوى تواجد العديد من علماء الاجتماع والأنثروبولوجيا أثناء الاجتماعات العشرة التي عقدة وقد كانت أبرز الشخصيات المتواجدة هي عالمة الاجتماع مارغريت ميد (Margaret Mead 1901 - 1978) والتي كانت تتقاسم رأي زوجها غريغوري باتيستون (Gregory Bateson 1904 – 1980) والذي يعد هو أيضا عالم في الأنثروبولوجيا، لقد كانت مارغريت تتقاسم وزوجها فكرة أن السبرانية، ستساعد على جلب منهجية وصرامة ودقة العلوم التطبيقية إلى العلوم الاجتماعية، كما أن النماذج التي تقدمها السبرانية يمكنها أيضا تفسير السلوك الإنساني، لأن الإنسان مثل أي كائن أو نظام مغلق، له مدخلات ومخرجات لتنقل المعلومات، وقد كان هذا يصب في عنوان المؤتمر

---

(240) Arturo Rosenblueth, Norbert Wiener, Julian Bigelow, "Behavior, Purpose and Teleology," in ***Philosophy of science association***, Volume 10(1943), pp. 18–24 .
(241) Ronald R. Kline, **op. cit**, p. 17.

الذي كان تحت عنوان آليات التغذية الاسترجاعية ونظام السببية الدائرية في علم الأحياء، والعلوم الاجتماعية.[242] فقد عملت مؤسسة مايسي على إشراك العديد من الباحثين اجتماعيين، وعلماء النفس، والعديد من العلماء في عدة مجالات، ذلك أن المعلومات ونظام المدخلات والمخرجات مرتبطة بكل التفاعلات الموجودة في المحيط، ومن اجل فهم هذه العلاقة يجب محاكات هذه التفاعلات عبر محاولة فهمها وتحليلها وتفسرها، ثم إعادة تنفيذها.

ولهذا يرى واينر أن عصر الحواسيب الرقمية، وأنظمة التحكم الآلي قد خلقت شيء جديد، حيث يقول **واينر**: [243]

"لقد خلقت الحواسيب الرقمية، عصرا جديدا من الاتصال والتحكم، وهذا يعد بمثابة الثورة الصناعية الثانية."

ولهذا يمكننا القول أن طرح واينر يوحي بأن القرن التاسع عشر، هو بمثابة عصر تحويل ونقل الطاقة، أما القرن العشرين، فسيكون بمثابة عصر تحويل ونقل المعلومات. [244] ولكن **واينر** وعكس **باوكرز** لم يقدم مفهوما عالميا للسبرانية رغم أنه درس السبرانية في العديد من المجالات، وأقرب تعريف قدمه **واينر** لعالمية السبرانية، هو لما عرفها على أنها: [245]

"مركب ومجمع علمي يتعامل مع الاتصالات والتحكم في الكائن الحي وفي الآلة."

لو نرى اليوم أين أصبحت الدراسات السبرانية، ونقوم بمقارنتها بالكتاب الأول الذي كتبه **نوربيرت واينر** حول السبرانية، سنرى أنه هناك فرقا شاسعا، فالكتاب الذي عالج فيه الموجات ومجموعة من المسائل العصبية التي تتعلق بالدماغ والتواصل، تحول فيما بعد إلى حقل واسع من الدراسات، فرغم أن واينر كان واعي بأن السبرانية سيكون لها مكان في الوسط العلمي حين قال: [246]

---

[242] ***Ibid***. p. 18.
[243] ***Ibid***. p. 29.
[244] ***Loc. cit***. p. 29.
[245] ***Ibid***. p. 116.
[246] Norbert Wiener, ***Cybernetics, or Control and Communication in the Animal and the Machine*** (The United States of America: Massachusetts, published by Massachusetts Institute of Technology, The 2nd edition, 1965), p. 6.

"الآن أرى انه حان الوقت لكي يتم اعتبار السبرانية، ليس فقط كجزء من تاريخ مستقبلي ممكن، ولكن كعلم قائم بذاته. "

إلا أن التطورات الذي أحدثتها وتوسع نطاقها كان غير متوقع، ولكن **واينر توفى** قبل أن يرى ذلك، ولعل أفضل صورة نمطية قدمتها السبرانية للأذهان، هو كتاب **دانيال هالسي** (Daniel Halacy 1919 - 2002) والمعنون بـ سايبورغ: تطور سوبرمان (Cyborg: Evolution of the Superman)، حين أراد أن يحذر ويقوم بتوعية القراء حول مخاطر تحول الإنسان إلى سايبورغ، ومن السايبورغ إلى السوبرمان أو الرجل الخارق، مؤكدا على أن البشر، دائما ما ربطوا انفسهم بالتكنولوجيا، وأصبح الآن الإنسان نفسه يمثل جزء من التطور في حد ذاته، فقد قام العلماء مؤخرا ما كان يعتبر من الخيال العلمي، إلى أشياء حقيقة.[247]

يمكننا أن نرى هنا أن السبرانية قد أصبح لها مداخل في العديد من العلوم، مثل ما هو الحال مع البيولوجيا، والهندسة، والعلوم الحاسوبية، وعلم الاتصال، وعلم الإدارة، وعلم الاجتماع، وعلم النفس، والطب، والفن، والأدب، والتقانة. حتى أن واينر، وفي كتابه الله و*الغوولام (God and Golem)، يناقش مسألة السبرانية والدين في مسألة الآلات التي يمكنها التعلم، والآلات التي يمكنها التكاثر، وفي الأخير تفاعل الآلات مع البشر.[248] كل هذه المداخل والطروحات التي تم ذكرها تساهم في خلق وعي وتوجه في البحث العلمي، خاصة في مجال تكنولوجية المعلومات، كأجزاء صغيرة يتم دراستها من اجل تركيبها معا فيما بعد، خاصة مع الإشارات المتكررة والواضحة إلى ربط السبرانية بما بعد الإنسانية، من اجل التعبير على محاولة فهم أعقد الأمور، من أجل محاكات أبسطها.

أما فيما يخص دراسة بحثنا هذا، فالتركيز سيكون أكثر على ما يسمى بالدراسات العلمية، التكنولوجية، الاجتماعية (technology and society - STS،Science)، وهي أحد أشكال الدراسات السبرانية (Metascience of Cybernetics)، والتي تدرس كيفية تأثير المخرجات السياسية والاجتماعية والثقافية، على البحث العلمي، والتقدم التكنولوجي، وكيف يمكن في المقابل لهذان الأخيران،

---

[247] Daniel Stephen Halacy, ***Cyborg, the Evolution of the Superman*** (The United States of America: New York, published by Harper & Row, the first edition 1965), p. 15.

• الغوولام (Golem) : هو كائن اصطناعي في الديانة اليهودية، وهو بمثابة رجل آلي مصنوع من الطين، وظيفته الأساسية هي الدفاع عن خالقه.

[248] Norbert Wiener, ***God and Golem Inc, a Comment on Certain Point Where Cybernetics Impinges on Religion*** (The United States of America: Massachusetts, published by M.I.T Press, the first edition, 1964), p. 11.

أن يؤثرا على المجتمع والسياسة. الأمر الذي يمكن أن يؤدي إلى تطبيق وإدراج أوسع للعلوم الأخرى داخل السبرانية. [249] كما سيؤدي أيضا إلى تقديم مقاربات لتحليل أعقد الأنظمة، من سُلم الخلية إلى السلم الاجتماعي.[250]الأمر الذي يمكن أن يجعل للسبرانية لغة عالمية يُتعامل بها ومتفق عليها.

السبرانية، وبعض النظر عن الأمن الإلكتروني، أو المخرجات العلمية لهذا التوجه الفكري، يوضح لنا شيء مهم هنا، وهو الدور الذي أصبحت تلعبه التكنولوجيا في الحياة الإنسانية، الدور الذي أصبح يترجم عبر تواجد التقنية في معظم حياة الإنسان العادي حاليا، هذه الثقافة التقنية أيضا، ستترجم بطريقة بديهية، وتتسع لتشمل أيضا باقي أنماط السلوك الإنساني، والذي يتعلق بحب السيطرة، أو الهيمنة، كما التسبب في الضرر للآخر، والبحث الدائم والمستمر على تحقيق الرغبات.

2.5.0 ما بعد الإنسانية:

إن أحد المفاهيم الجديدة التي أصبح لها تواجد متزايد ومستمر في حل التطور التقني والمعلوماتي، هي بروز ما يسمى بـ ما بعد الإنسانية (Transhumanism)، يمكننا أن نقول أن التكلم على ما بعد الإنسانية، هو التكلم على معظم المحاولات التاريخية، والأفكار الفلسفية، أو العلمية، والتي كانت تبحث على سبل تحرير الإنسان من هاجس الموت أو تمديد المدة التي يمكن أن يعيشها الإنسان، كما تحسين ومعالجة الأخطاء التي يمكن أن يعاني منها الإنسان، فموضوع ما بعد الإنسانية يشكل ذلك التجمع الكبير من الأفكار الذي اصبح يربط العديد من العلوم ببعضها البعض، كما يركز أكثر على العلوم، والأفكار التي يمكنها أن تخدم الكائن البشري، بطريقة تسمح له، بأن يتعدى حدود قواه الحالية، إلى مراحل متقدمة من القوة، والقدرات.

لو ألقينا نظرة على التاريخ، يمكننا أن نرى أن الإنسان لطالما بحث عن طريقة في تمديد حياته، أو القضاء على هاجس الموت، ولهذا، فهو دائما كان ينظر إلى الموضوع، ويبحث فيه، ويعبر عن هذه الرغبة، فحتى إذ نظرنا إلى ما يعتبره العلماء اليوم، أقدم قصة في التاريخ، نجد أنها تتكلم على موضوع الأبدية، وهذا فعلا ما حصل في كتابات ملحمة جلجامش التي كتبت سنة 2100 قبل الميلاد في منطقة العراق حاليا (Epic of Gilgamesh 2100 BC)، والتي جلجامش فيها يبحث عن الأبدية عبر القيام

---

[249] Ronald R. Kline, **op. cit**, p. 62.
[250] ***Ibid***. p. 100.

بإنجازات عظيمة للآلهة،[251] وعلى مر العصور، ارتبط هذا التساؤل بالعديد من الدراسات العلمية التقليدية، مثل ما هو الحال مع الأبحاث التي قام بها العديد من العلماء في مختلف الحضارات القديمة في ما كان يسمى *بالخيمياء (Alchemy)،[252] ولكن الخيمياء أصبحت تعتبر حاليا من العلوم الزائفة (Pseudoscience) عكس البحث عن الحياة الأبدية، إذ أن هذه الفكرة، لطالما ارتدت على أذهان المفكرين والباحثين في كل عصر، وقد عبرت كل قفزة تكنولوجية على هذا النمط من التفكير، كوننا قادرين على إيجاد مثل هذه الأفكار في العديد من الكتابات على مر التاريخ، وإلى يومنا هذا.[253]

ولهذا، أصبح ينظر إلى ما بعد الإنسانية حاليا، على حقل يدرس كل ما هو فلسفي ، وعلمي في نفس الوقت، إذ انه يدرس القضايا التي تتعلق بالإنسان، والقضايا الأخلاقية التي تشكلها هذه القفزة في التفكير، كما الدراسات التي تتعلق بعلم الأعصاب، والعديد من العلوم التطبيقية الأخرى التي تدرج تحت هذا الحقل المعرفي الموجه أكثر نحو التقانة الحيوية (Biotechnology)، والتي تعد أحد فروع علم الأحياء (Biology) التي تشير إلى أي تطبيق تكنولوجي يستخدم أنظمة حيوية من أجل القيام بتغييرات معينة في المنتجات، أو العمليات أو أي استخدامات أخرى.[254] لهذا ووفق ما سبق، يمكننا أن نعبر على ما بعد الإنسانية على أنها:[255]

"تلك الحركة العالمية، والتي تعالج قضية التطور، والتي تركز على استعمال التقانة للتفوق على الحدود الطبيعية للقدرة الإنسانية".

لقد أصبحت التكنولوجيات الناشئة (Emerging technologies) أحد أبرز مظاهر العصر الحالي، إذ أن التحكم المتزايد في الموارد الطبيعة، جعل من الاستخدامات الصناعية، والعسكرية، والتجارية للعديد من المواد الأولية، أو الاختراعات، والتي لم تكن ذات مردودية كبيرة في حال الإنتاج

---

[251] Penguin Classics, N. K. Sanders, **The Epic of Gilgamesh** (United Kingdom: London, Published by Penguin Books, Kindle Edition, 1973), pp. 61-125.

- الخيمياء (Alchemy): علم قديم، ومعاصر عند بعض الباحثين، يبحث في علم الفلك، والفلسفة، والرياضيات، والطب، والكيميا. وتحويل المعادن؛ حيث كان يعتقد بقدرة تحويل بعض المعادن إلى ذهب.

[252] Joseph P. Farrell, Scott D. Hart, **Transhumanism, A Grimoire of Alchemical Agendas** (The United States of America: Washington, published by Feral House, the first edition, 2011), pp. 5-16.

[253] Nick Bostrom, "A History of Transhumanist Thought," in ***Journal of Evolution & Technology***, Volume 14(April, 2005), pp. 1-24.

[254] United Nation, ***Convention on Biological Diversity***, 1992, p. 4.

[255] R. U. Sirius, Jay Cornell, **Transcendence: The Disinformation Encyclopedia of Transhumanism And The Singularity** (The United States of America: San Francisco, published by Disinformation Books Red Wheel/Weiser LLC, the first edition 2015), p. 3.

على نطاق واسع(Mass production) شيء يمكن التعامل معه من جديد من أجل تحقيق الفائدة، أو المصالح؛ فالذي يهمنا هنا، هو التطبيقات العسكرية، خاصة تلك التي لها علاقة بالإلكترونيات، والتقانة المتطورة، فالتكلم على ما بعد الإنسانية حاليا، خاصة بعد الإنجازات العلمية الكبيرة التي حدثت، يجعلنا في نقاش حول التقدم أو الذروة التي تحصل كل قرون، الذروة التي تجعل الإنسانية يكتشف شيء جديد يشكل نقلة (Transcendence) نوعية في طريقة عيشه، وهذا ما عبر عليه الباحث، والكاتب، والمهندس، والعالم في المستقبليات **ريموند كرزويل** (Raymond Kurzweil)؛ فرغم أن الهندسة العكسية لقدرات الدماغ عملية ليست دقيقة تماما، لكن ريموند يرى أنه في فترة معينة، ستتفوق القدرة الحاسوبية على دماغ الإنسان، أي تبرز وحدات ذكاء تتوفق على الإنسان (Superintelligence)،[256] إذ سيحدث ما اسماه الانفجار التكنولوجي (Intelligence Explosion) الذي سيؤدي إلى الوحدة التقنية أو الوحدة التكنولوجية (Technological Singularity)، والتي تعبر على جيل تصبح فيه للحواسب قدرة على الإدراك، والتعامل، والتطور، والبناء بطريقة مستقلة. لكن يجب أن نقول أن هذه الفكرة لا يتقبلها الجميع، فقد عبر العالم الهولندي في الرياضيات والحاسوب **ادسخر ويبي ديكسترا** (Edsger Wybe Dijkstra 1930-2002) على مثل هذه الأفكار حين قال:[257]

"**إن السؤول الذي يبحث عن إمكانية أن يكون للحاسوب قدرة للتفكير، لا يعد أكثر أهمية من السؤال حول قدرة الغواصة في السباحة**".

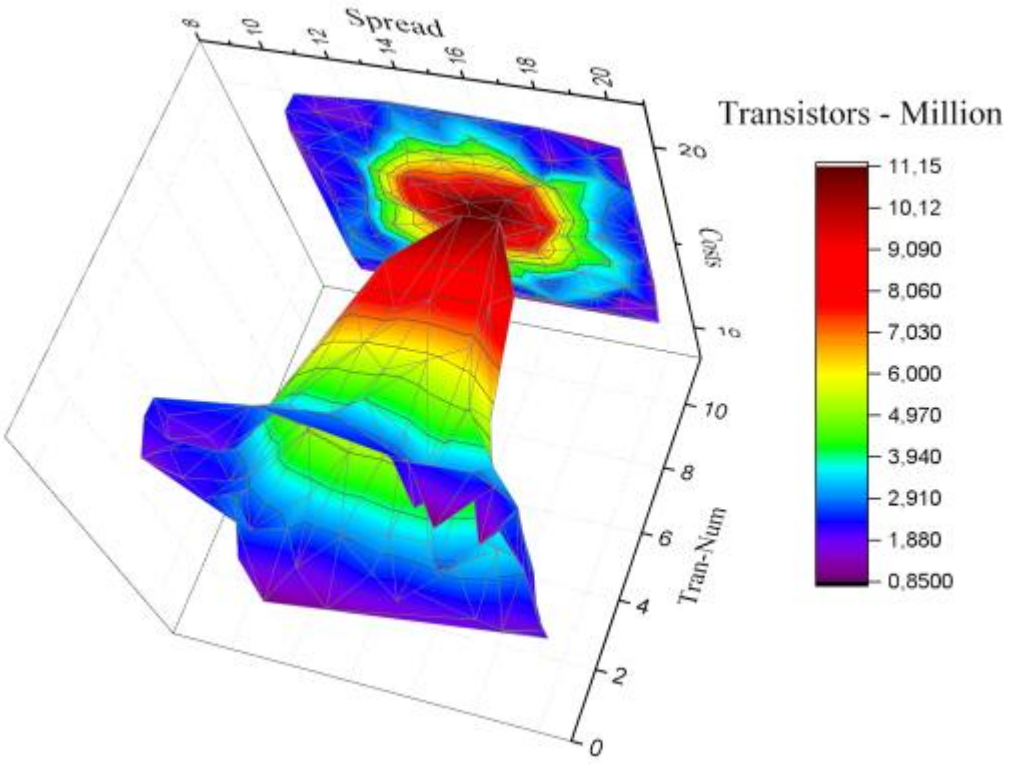
مثل هذه الأسئلة التي تطرح تبين لنا طبيعة تغير التفكير الإنساني كما رأيناه سابقا في أجيال الحروب، فالثقافة، والتقانة، دائما لديها دور في تحريك الإبداع البشري ودفعه إلى طرق محددة، ومعينة من اجل البحث فيها، ويمكننا أن نقول أنه ووفق بعض هذه التساؤلات، فالإنسان يرى عالم المستقبل، كعالم افتراضي، إلكتروني، ميكانيكي، آلي، أين معظم أشكال الحياة الإنسانية تصبح قابلة للمحاكات.

---

[256] Bill Joy, "Why the future doesn't Need Us," in: ***http://qoo.gl/1uFywu***, (Thursday, May 05, 2016).

[257] Amnon H. Eden, James H. Moor, Johnny H. Soraker, Eric Steinheart , **Singularity Hypotheses, a Scientific and Philosophical Assessment** (United Kingdom: Clochester, the School of computer Science, published by Springer Verlag Berlin Heidelberg – Dordrecht London, 2012), p. 216.

الشكل رقم: 2.1



شكل افتراضي يوضح تطور القوة الحاسوبية، واقترابها إلى قيمة

كرزويل للوحدة التكنولوجية(singularity). (من إعداد الطالب)

يمكننا أن نرى اليوم العديد من النماذج التي تعمل على تحسين القدرة الإنسانية، ويمكن رؤية أن هذه النماذج، منها ما له تطبيقات عسكرية أساسية، والجانب الآخر يمكن أن يكون لأغراض بحثية، تتعلق بحسين الظروف الإنسانية بشكل عام؛ ففي سنة 2013 أعلن الأميرال الأمريكي **وليام ماككريفن** (McRaven William) عن ما يسمى : بدلة العمليات الخفيفة للهجوم التكتيكي باختصار* تالوس (Talos - Tactical Assault Light Operator Suit)،[258] هذه البدلة ستكون ثمرة تعاون العديد من الشركات المتخصصة في التقنيات المتقدمة، والعديد من الحكومات في العالم، والجامعات المتخصصة أيضا، هذه البذلة ستعطي للجندي قوة إضافة، وسرعة إضافة، كما ستحميه من الذخيرة من المستوى الثانية بفضل سائل ممغنط خاص (Magnetorheological Fluid)؛ مثل هذه المساهمات

[258] Samantha Dean, "The U.S Army Is Building an Iron Man Suit for Soldiers," in: ***http://goo.gl/nkTToD***, (Friday, May 06, 2016).

- تالوس (TALOS): في الميثولوجيا الإغريقية، تالوس عبارة عن عملاق برونزي، صنعه هيفيستوت(Hephaestus)، ابن زوس(Zeus)؛ مهمته الأساسية هي حراسة جزيرة الكريت اليونانية.

تبين لنا فعلا رغبة الاتحاد في تعدى الحدود التي تفرضها الطبيعة عليه، ولكن ذلك لا يتوقف فقط على الاستخدامات العسكرية، إذ يمكننا أن نجد مثلا العديد من الإنجازات التي هي قيد التطوير في جامعة بتسبرغ (Pittsburgh)، خاصة تلك التي تتعلق بربط مُرَكبات آلية متحركة، والسماح للعديد من الأشخاص المعاقين، أو المشلولين، أو المبتورين، بالتحكم بذراع آلية يتم التحكم فيها فقط عبر التفكير، محدثين بذلك ثورة فعلية في هندسة الإلكترونيات الحيوية (Bionics)، والجراحة الترقيعية المتقدمة (Advanced Prosthetic). [259]

لقد قلنا من قبل أن الخيماء أصبحت تعتبر من قبل العديد على أنها علم غير صحيح، ولكن يمكننا أن نرى حاليا، وخاصة بتقنية تحويل المعادن التحليلية (The Synthesis of Precious Metals)، تم تحويل الزئبق إلى ذهب، لكن التقنية لا يتم استعمالها بسبب أن تكلفة الإنتاج تتعدى قيمة الذهب، من جانب آخر، أصبحت هناك الخلايا الجذعية (Stem Cell) التي جعلت من بناء الأعضاء شيء ممكن وقابل للإنجاز؛ الشيء الذي يميز كل هذه الطفرات العلمية، هي القاعدة الإلكترونية، والحاسوبية لهذا العلم، فمؤخرا، أصبحت الدراسات المعمقة في مجال البروتينات مثلا، تحتاج إلى قدرة حاسوبية كبيرة، ولا يخفى على أحد أنه من يسيطر على العلم والتقانة، فإنه يسيطر على العالم، مثل هذه الطفرات أصبحت تشكل في العديد من الحالات موضع خطر، وصراع فعلي، مثل ما حدث مع قضية البصمة الزرقاء لطائرة إف–35 التي اتهمت الولايات المتحدة الأمريكية الصين بأنها قامت بسرقتها عبر استخدام قراصنة، خاصة أن سندون اكد ذلك أيضا. إذا كانت ما بعد الإنسانية هي بمثابة فلسفة تدفع الناس إلى الاختراع والبحث، فإن امتلاك القوة والهيمنة في العلاقات الدولية، شيء لا يمكن الهروب منه، ففي ظل هذه المحورية والاختلاف في القدرات العلمية، برزت تكنولوجيات الاتصال كوسيلة لكسر هذه الهيمنة العلمية، عبر توفير الموارد العلمية للجميع وللعامة، عبر قرصنتها أو تسريبها، أو جعلها مفتوحة المصدر، هذه العملية غير مرحب بها من قبل الجميع، وقد وقعت العديد من الأحداث التي دخل فيها أشخاص السجن بسبب قرصنتهم لوثائق علمية تقدر بالملايين الدولارات، ولهذا، يمكننا القول أن المخرجات التطبيقية التي تعد بها ما بعد الإنسانية، ستكون محل للصراع بين القوى العالمية، كون هذه المخرجات تعبر عن التفوق الإنساني على الطبيعة، هذا التفوق، سيترجم مثل ما بينه التاريخ، إلى وسائل جديدة، واستراتيجيات، وطرق جديدة، للصراع، والهيمنة الدولي.

---

[259] Michael M. Bridges, Matthew P. Para, Michael J. Mashner, "Control System Architecture for Modular Prosthetic Limb," in **JOHNS HOPKINS APL TECHNICAL DIGEST**, No 3, Volume 30(November, 2011), pp. 217-222.

2.6 الحقول المتداخلة

لقد تكلمنا في السابق، وخاصة في موضوع السبرانية على قضية التوجه الجديد الذي له علاقة بالحقول المتداخلة (Interdisciplinarity)، وإمكانية الخروج بنتائج أكثر شمولية لما يشارك أشخاص من عدة تخصصات من أجل الخروج بنتائج معينة. فحاليا وخاصة مع التصاعد المستمر للدور الذي اصبح تلعبه التقانة في العلاقات الدولية على عدة أصعدة، أصبح من الواضح جدا، انه من اجل فهم هذه الظاهرة الجديدة، والتي أصبحت تمس كافة الحياة الإنسانية، وعلى مختلف الأصعدة، يجب علينا على الأقل معرفة الحقول التي أصبحت لها علاقة مباشرة بالموضوع، وارتدادات هذه التحولات على حقول التدريس، لقد أصبحت هناك نظرة جديدة حول التعاطي مع العلوم، رغم أن هذه النظرة لا تعد جديدة، بل يمكن اعتبارها بمثابة، الالتقاء الجديد للعلوم؛ ولهذا أردت أن نطرح هنا بعض الأفكار التي لها علاقة بهذه المقاربة، والتي تعد على المستوى المنهجي أحد اهم الطرق التي أصبحت تعتمد في مجال الأمن الإلكتروني، أو الحرب الإلكترونية، كون التعامل مع مثل هذه القضايا، وخاصة لما اصبح للأمر علاقة وطيدة بالحياة الإنسانية، بالثقافة الإنسانية، بالتبادلات الاجتماعية، بالنمط الجديد الذي أصبح يشكل معنى أن يعيش الشخص.

فكما كنا قد وضحنا ذلك سابقا، يمكن القول أن هذه العملية قد فرضت نفسها، ونفس الوقت، لا يجب اعتبارها أنها عملية جديدة، فمثل هذا التكامل المعرفي يعد أحد أحجار الزاوية الذي يسمح بالتقدم المعرفي والعلمي، ولكن الوتيرة أصبحت مؤخرا أكثر إلحاحا في ظل الترابطات الكبيرة التي أصبحت موجودة خاصة في مجال الأمن الإلكتروني، أو هذا العصر الرقمي، فالحقيقة هنا أنه هناك من العلماء من يرى أن قضية تقسيم المعرفة بالطريقة التي نعرفها اليوم، تعود إلى إسهامات قديمة خاصة مع الفلاسفة الإغريق: **أريسطوكلس** (Aristocles Son of Ariston 423/424 BC -347/348 BC)، و**أرسطو** (Aristotle، son of Nicomachus 384 BC- 322 BC)، ولكن من جانب آخر وخاصة مع بداية الثورة العلمية في أوروبا، هناك من رفض هذه التجزئة العلمية في التخصصات مثل ما هو الحال مع فرانسيس بيكون (Francis Bacon 1561-1621)، كذلك العديد من النماذج في الحضارة الإسلامية التي كان يتميز علمائها بالموسوعية (Encyclopedic knowledge). [260]

---

[260] هايدي ليدفورد، "التخصصات المتداخلة: لماذا يجب على العلماء أن يعملوا مع لإنقاذ العالم"، **الطبيعة**، العدد 38(نوفمبر، 2015)، ص ص. 93-94.

يجب أولا معرفة أن التعامل مع الشخصيات المختلفة ضرورة لا بد منها من أجل تشجيع روح الاكتشاف، والإبداع، ; العمل بطريقة فعالة ، وأصبح العمل على مهارات القيادة عند مختلف الدوائر البحثية، الصغيرة منها، أو الكبيرة، شيء يُشجع على فعله؛[261] فإن التعامل من جانب آخر مع تخصصات مختلفة ،ومتعددة، يتطلب المستوى نفسه من الاجتهاد والاستثمار، خاصة أنه هناك من يعتبروا أن قضية التخصصات المتداخلة لا تتعدى سوى ضم مجموعة من السير الذاتية، ولكن بذلك، يكونوا قد أزاحوا العامل البشري في المعادلة، إذ يجب معرفة أن بناء علاقة شخصية في الأوساط العلمية تتطلب الوقت،[262] ففي أي محاولة جديدة لإدخال مناهج، أو طرق جديدة للتحليل أو التدريس، فإن الأمر يحتاج إلى الوقت من أجل القيام بذلك، ومن اجل بناء أرضية بين مختلف الباحثين والتخصصات ومحاولة لإيجاد لغة مشتركة تساهم في إثراء القضية التي تتم معالجتها.

ففي العدد 38 من مجلة الطبيعة (Nature) سنة 2015 باللغة العربية، تتكلم **شارون ديري** (Sharon Dairy)، المتخصصة في علم النفس التربوي في جامعة كارولينا الشمالية في تشابل هيل، والتي تدرس التخصصية المتداخلة ، وتقول:[263]

> "**إن مشكلات العالم لا تقع ضمن تخصص واحد.. علينا أن نجمع ذوي المهارات والخبرات المختلفة معًا.. فلا أحد يملك كل ما هو مطلوب للتعامل مع القضايا التي نواجهها**".

لقد تم طرح هذا التداخل على عدة مستويات، هذا إلى جانب العديد من الصعوبات، والمشاكل، والتحديات التي واجهت هذا الطرح الذي هو في انتشار متزايد، كما بعض الصعوبات التي تواجه بعض العلماء مثل علماء الاجتماع في الاندماج بسبب بعض النمطيات الذهنية التي تتعلق بالدقة في المعلومات. هذه النظرة الجديدة للتعاطي مع البحث العلمي خاصة بعد الحرب العالمية الثانية، سمحت بالعديد من الاختراعات والاستنتاجات العلمية والمجتمعاية. فدراسة الأمن مثلا وكل الأسس والخلفيات

---

[261] تشارلز إي لايسرسون، تشاك ماكفيني، "يحتاج أساتذة العلوم إلى تدريب على مهارات القيادة،" **الطبيعة**، العدد 36(سبتمبر، 2015)، ص ص . 39-41.

[262] هايدي ليدفورد، ***مرجع سابق***.

[263] نفس المرجع.

والوسائل التي يعتمد عليها لم يعد فقط يقتصر على الدراسات السياسية، والمجتمعاتية، للعلاقات الدولية، وأسباب الصراع، بل أصبحت دراسة هذه الصراعات، والمتطلبات الأمنية تعد ظاهرة اكبر يجب فهمها عبر فهم اكبر لمختلف التفاعلات، والاتصالات بين مختلف العلوم، والهدف هنا ليس وضع قاعدة شاملة، ونهائية مثل ما ينظرون إليه أصحاب *نظرية الحقل الواحد (Unified Field Theory)، وإنما البحث على أنساق معينة مشتركة تزودنا بمعلومات من اجل فهم فعلي لما أصبح يمثله الأمن الإلكتروني للإنسان.

هذا الطرح لم يوضع فقط من اجل معالجة بعض المواضيع التي يجب معالجتها، أو هي قيد اهتمام بحثي لأي سبب كان، بل يطرح أيضا على مستوى التدريس، ذلك أن مثل هذه المقاربة ستسمح بانتعاش أكثر أثناء الدراسة، وذلك باعتبار الأشخاص الذين هم قيد التعلم ليسوا فقط كوحدات متلقية، بل أيضا كوحدات مؤثرة، يمكن أن تؤثر، بحكم عملها، أو تخصصها، أو ميولاتها أو ثقافتها؛ ونجد في هذا الصدد أن الأستاذ والباحث الكوري الجنوبي **تاي إيوج لي**، له فلسفة بسيطة بشأن ما يجب أن يقوم الأكاديميون في المحاضرات، والتي تتمثل في أنهم يستطيعون القيام بأي شيء، عدا أن يحاضروا، ويقول في هذا الصدد تاي إيوج:[264]

"**عـادة، فـي الفصـول الدراسـية التقليديـة، نجـد أن الطـلاب لا يفكـرون. إنـهم يتبعون فقط تدريس الأستاذ**".

لذلك وفي جامعة معهد كوريا المتقدم للعلوم والتقنية (KAIST) في ديجون، في كوريا الجنوبية، حيث يرأس مركز التميز في التعليم والتعلم، يعمل **تاي إيوج** على تنفيذ مفهوم الفصل الدراسي المقلوب، فبدلا من الجلوس في محاضرات أحادية الاتجاه لا تنتهي، يشاهد الطالب الدروس عبر الأنترنت في المنزل، ثم يأتون إلى الفصول من اجل لمناقشة الأفكار، والعمل على حل المشكلات في مجموعات صغيرة، المعيدون والمشرف هناك للإشراف، لكن معظم التعلم يحدث فيما بين الطلاب أنفسهم. ويسمي

---

[264] مارك زاسترو، "كوريا الجنوبية: الجامعة المقلوبة،" **الطبيعة**، العدد 27(ديسمبر، 2014)، ص ص. 39-40.

- نظرية الحقل الموحد (Unified Field Theory): نظرية تحاول توحيد القوى الأساسية في الكون في نظرية واحدة متكاملة، وذلك عبر محاولة إيجاد العلاقة الترابطية، بين أربعة قوى أساسية في الكون المعرفة، وهي الجاذبية(Gravity)، والقوة النووية الضعيفة(Weak Interaction)، والكهرومغناطيسية(Electromagnetism)، والتآثر القوي(Strong Interaction).

إيوج لي هذه العملية، بالجيل الثالث من التعليم (Education 3.0)، ويراه طريقا لإثارة الإبداع والعمل الجماعي. وكانت نتيجة هذه العملية أن حوالي 71% من الطلاب الذي شاركوا في المحاضرات المقلوبة، عبروا عن تحسنهم في فهم المواد، وزيادة في الحافز الدراسي، والتركيز لديهم. وقد نجحت هذه الطريقة في التعليم وهي في توسع مستمر لدرجة أن **سانجاي صارما** (Sanjay Sarma)، وهو مدير المعهد الرقمي في ماساتشوستس صراح وقال:[265]

"**إنهم يغيرون ثقافة التعليم على نطاق واسع.**"

إن عدم التركيز على المهارات التي ستسمح للخبراء والباحثين على توسيع مهارات القيادة لديهم، وكذا اندماجهم في هذه المحاولة التي تهدف إلى دمج مختلف الأشخاص تحت مضلة واحدة، ستؤدي سواء بوجود تعدد الخبراء، أو لا، إلا أن الفرق الأكاديمية تصبح تضيع الوقت في التعامل مع مسائل شخصية غير مفيدة، وغير مهمة، كما ينقص الحماس وتتطور العديد من الأوضاع الحرجة إلى نزاعات، تكون تكلفتها باهظة، من حيث الميزانية، والمواهب أيضا. ولكن رغم هذا، يؤكد كل من الأستاذ في علوم الحاسوب والذكاء الاصطناعي في معهد ماساشوستس تشارلز لايسرسون(Leiserson Charles)، ورئيس شركة ماكفي للاستشارات الإدارية تشاك ماكفي(Tchack Makfini) أنه:[266]

> "**على الرغم من أن إقناع الأساتذة بالتغير أمرا لا تخفى صعوبته، فثمة مؤشرات تشير على أن الأمور في تحسن، فعلم العمل الجماعي، هو مجال دراسة ينمو سريعا، ويهف إلى مضاعفة كفاءة البحث المعتمد من قبل فرق البحث في كافة العلوم**".

ولهذا أصبح للكاريزمية في القيادة أهمية كبيرة من اجل إنجاح أي عملية لها علاقة بالأشخاص كما يقول العالم في السياسية، والاقتصاد، وعلم الاجتماع، **ماكس ويبر**(Maw Weber 1864-1920)، كون

---

[265] مارك زاسترو، ***مرجع سابق***، ص ص. 39-40.

[266] تشارلز إي لايسرسون، تشاك ماكفيني، ***مرجع سابق***، ص ص. 39-41.

الكاريزما بمثابة حجر ممغنط تدور حوله الأحجار الأخرى،[267] بل يمكننا أن نجد أنه حتى الباحثة في علم الاجتماع، والسياسية **آنن روث ويللنار**(Ann Ruth Willner)، تؤكد على هذه الفكرة حين تقول حين تقول:[268]

"**الأمـر لا يتعلـق بماهيـة القائـد ومـاذا يمثـل، بـل الأمـر يتعـل فـي كيفيـة رؤية الناس للقائد**".

من هنا يمكننا أن نفهم، ما أصبحت تمثله الحقول المتداخلة في هذا العصر، فالثورة العلمية، والتكنولوجية، جعلت التعاطي مع العلوم، والمخرجات التي تقوم عليها، تستوجب النظر إلى الظاهرة العلمية بطريقة مختلفة، هذه التغيرات لا تعد شيء جديد، بل شيء كان موجود من قبل، ولكنه فرض نفسه مؤخرا، فالتكامل الموجود في الطبيعة انعكس على طريقة التدريس ورؤيتنا للعالم، فإذا كنا من قبل نرى أن صناعة آلة معينة تقتضي فقط التمكن من قطاع علمي معين مثل الميكانيك، أصبح ذلك غير ممكن في الوقت الحالي، وذلك ليس بسبب طبيعة الآلة التي يتم صنعها، وإنما التطورات المجتمعية والسكانية التي حدثت، جعلت من التطور التقني أهم بديل يعتمد عليه من أجل تلبية الحاجة الإنسانية، وتلك الآلة الميكانيكية البسيطة، لم يعد بإمكانها تلبية، وتوفير، وتغطية الرغبات المتزايدة للبشر؛ لذا برزت تقانة متطورة جديدة، معقدة، ومركبة، ويصعب تصنيعها من قبل شخص واحد، أصبحنا الآن نعتمد على الإلكترونيات، أكثر من اعتمادنا على العنصر البشري، لقد وصلنا حاليا إلى ما يسمى بعلم الاجتماع الآلي (Computational sociology - Computational social science)، والذي يجمع بين علم الاجتماع وعلم الحاسوب، إذا أصبحنا نعتمد أكثر فأكثر إلى الآلة كوسيلة تفاعل اجتماعية، وكي يتوفر ذلك، سنحتاج إلى أشياء أكثر من مجرد الميكانيك التقليدية؛ وفي هذا الصد يمكننا ذكر القواعد الثلاثة الشهيرة التي جاء بها المؤلف، والأستاذ، والكيميائي : **إسحاق أسيموف** (Isaac Asimov 1920-1992)، حين قدم هذه القوانين في الرواية التي نشرها سنة 1942 تحت عنوان: الهارب

---

[267] Max Weber, ***The Sociology of Charismatic Authority: Essays in Sociology Trans*** (The United States of America: New York, published by Oxford University Press, the first edition from the original essay in German (1921), 1964.), pp. 245-252.

[268] Ann Ruth Willner, ***The Spellbinders, Charismatic Political Leadership*** (The United States of American, Connecticut, published by Yale University Press, the first edition, 1984). p.14.

(Runaround)، وتم تحديد طرحه في سلسلته للخيال العلمي تحت عنوان: أنا، روبوت (I Robot) سنة 1950؛ وتنص هذه القوانين على:[269]

1. لا يُسمح لآلي أن يؤذي البشر، أو أن يسبب عدم فعله لشيء ما، الأذى للبشر أيضا.
2. على الآلي إطاعة أوامر البشر، بشرط أن هذه الأوامر لا تتعارض مع القاعدة الأولى.
3. يجب على الآلي الحفاظ على بقائه، بشرط أن هذه العملية لا تتعارض مع القاعدة الأولى، والثانية.

ثم أضاف أسيموف قاعدة أخرى إلى بقية القواعد، وهي القانون الأساسي: صفر (Zeroth Law) الذي يأتي قبل كل القوانين السالفة الذكر، نشر هذا القانون لأول مرة سنة 1985 في رواية أخرى كتبها تحت عنوان: الآليين والإمبراطورية (Robots and Empire)، وينص هذا القانون على:[270]

0. لا يُسمح لآلي بإيذاء الإنسانية، أو أن يسبب عدم فعله لشيء ما، الأذى لها أيضا.

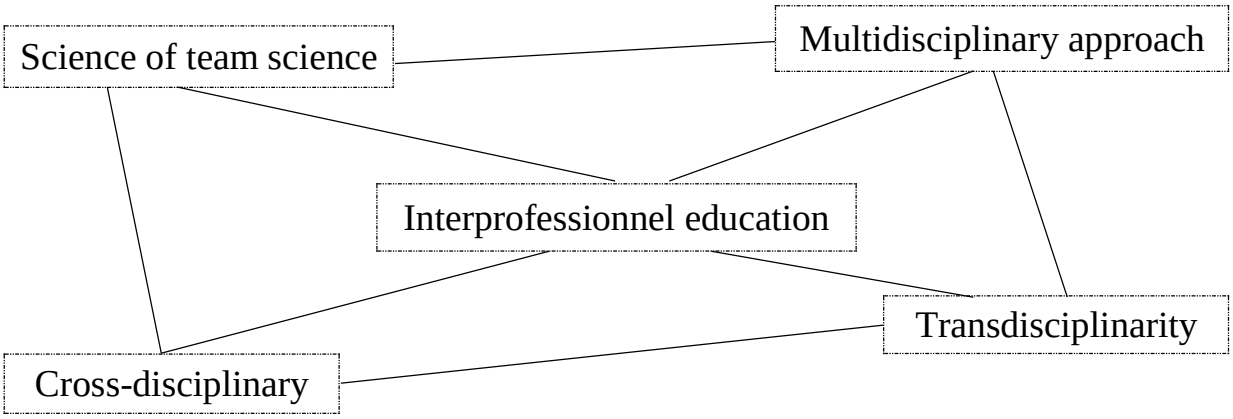
لقد راينا هنا نموذج عن طريقة التفكير التي أصبح يفكر بها الناس في العصر الرقمي، ومما بدأ كشيء افتراضي أصبح يجسد كحقيقة تدرس، حقيقة أن الآلة ستكون جزء من حياة الإنسان ولا يمكن فصلها، ونحن لا نتكلم هنا عن الآلة التي تقوم بعمليات حسابية فقط، بل الآلة التي تقوم بمحاكات السلوك الإنساني، ولن نبتعد كثيرا هنا لو قلنا أن هذا الأمر سيطلب أكثر من اختصاص للقيام بذلك، لهذا يمكننا أن نجد حاليا العديد من المفاهيم التي تعبر عن هذا التداخل المعرفي وأهميته، مثل ما هو الحال مع: الدراسات العبرمنهاجية (Transdisciplinarity)، والمقاربات البحثية المتعددة التخصصات (Multidisciplinary Approach)، والعابرة للتخصصات (Cross-disciplinary)، والدراسات المتكاملة (Integrated Studies)،[271] وعلم الفرق العلمية (Science of team science).[272] فاعتماد بعض من المفاهيم المذكورة سالفا، ستطور التفكير النظمي (Thinking Systems) لدى أي شخص، الأمر الذي سينعكس بشكل كبير جدا على كفاءته في التحليل ، والتفكير ، كما على قدرته في بناء تقانة ذو أجيال متقدمة، خاصة مع التقانة التي تعتمد على الكثير من التخصصات المعقدة مثل ما

---

[269] Isaac Asimov, ***Runaround, in I, Robot Collections*** (The United States of America, New York, published by Street and Smith Publications, Inc, the first edition, 1942), p. 26.
[270] Isaac Asimov, ***Robots and Empire*** (The United States of America, Ney York, published by Doubleday, the first edition, 1985), p. 285.
[271] Suzie Boss, "Integrated Studies: A Short History," in: ***http://goo.gl/uNoeRm***, (Wednesday, April 27, 2016).
[272] Daniel Stokols, Kara L Hall, Brandie K Taylor, Richard P Moser, "The Science of Team Science: Overview of the Field and Introduction to the Supplement," in ***American Journal of Preventive Medicine***, No 2S, Volume 35(August 2008), pp, 77-89.

هو الحال مع هندسة الميكاترونيات (Mechatronic)؛[273] والتي تعمل مثلا على دمج الإلكترونيك، والميكانيك، والهندسة الحاسوبية، والإلكتروميكانيك، وأنظمة التصميم، والروبوتيك.[274]

الشكل رقم: 2.2



شكل يوضع بعض أشكال الحقول المتداخلة. (إعداد الطالب)

التخصصات المتداخلة لا تطرح تحديا من حيث المنهجية، وطريقة العمل فقط، بل تطرح تحديا من مستوى آخر، إذ لقد طُرحت العديد من التساؤلات حول القدرة الإنسانية على الاستيعاب، وإمكانية تمكنه من فهم، واستيعاب الترابطات الموجودة بين العديد من التخصصات في آن واحد؛ فهناك العديد من الدراسات التي طرحت مؤخرا عدة اقتراحات تقول على أن ذاكرة الإنسان القصوى يمكن تقديرها بين 100

[273] Martin Slavík, "Mechatronics Studies in Europe," in: ***http://goo.gl/u2hWfT***, (Thursday, April 28, 2016).
[274] Carence W. de Silva, ***Mechatronics, a Foundation Course*** (The Unites States of America: New York, published by Taylor & Francis Group, the first edition, 2010), pp. 1-2.

جيجابايت إلى 10.000.000.000 جيجابايت (1 مليار× 10)،[275] مع قدرة فائقة في تحليل البيانات تصل حتى إلى 38 بيتافلوب (Petaflop)(1 مليار ×38.000.000.000.000)، أي ما معدله بالتحديد

380.000.000.000.000.000.000.000 تريليون عملية في الثانية. [276] ولهذا، فالذاكرة لا يمكنها أن تُحَصل كل شيء، وسيصل الإنسان إلى الحد الذي سيتوجب عليه التخصص وفقا لمصالحه، لكن ذلك الحد لم يصل إليه أحد بعد.

في نهاية دراستنا لإطار النظري، الذي يهمنا هنا، هو أنه من ناحية، أصبح من الصعب جدا التكلم على الأمن، وبالأخص الأمن الإلكتروني، بغض النظر على الأعصاب التي يقوم عليها، كون أن الأمن تغيرت معاييره من حيث المضمون، والوسيلة، والمعني بتحقيق الأمن أيضا؛ لم نصبح في ذلك القرن الذي كان فيه المجرم، لا علاقة له بالعلم، أو التحصيل العلمي، لقد أصبحنا بعيدين عن ذلك العصر الذي كان فيه الخارج على القانون، هو ذلك الشخص الذي يعاني من نقص في العلم، والمعرفة، والذي يعاني من ظروف إنسانية معينة؛ نحن الآن في جيل جديد من العلاقات الاجتماعية، جيل جديد من ضوابط القوة، حين اصبح فيه، أعلم الأشخاص، هم أكثرهم خروجا على القانون، وهذا الشيء هو الذي يميز الصراع الإلكتروني العالمي، ففي ظل تحول المعرفة إلى معرفة مفتوحة، أصبحت هذه الوسائل لإلحاق الضرر متاحة للجميع، ويمكن لأي شخص أن يعتمدها من أجل التعبير عن رغبة معينة أو إبداء راي معين، فلا يجب التعجب لما نرى أن اكبر عمليات القرصنة في العالم، وأخطرها، مثل ما هو الحال مع القرصان الوحيد(Solo) **غاري ماكينون** (Gary McKinnon)، والذي يعد أكبر قرصان عبر التاريخ كونه قام بأكبر عمليات قرصنة عسكرية في تاريخ القرصنة الإلكتروني؛[277] والأهم من هذا هنا هو معرفة أن ماكينون لم يكمل الدراسة، وكان عصامي التعلم، وكان قد أستعمل وسائل جد بسيطة من أجل القيام بذلك، فإذا كان

---

[275] Matthew Hutson, "How Much Can Your Brain Actually Process? Don't Ask,"in: ***http://goo.gl/sornMi***, (Wednesday, April 27, 2016).

[276] Larry Greenemeier, "Computers have a lot to learn from the human brain, engineers say," in: ***http://goo.gl/dOW0sB***, (Wednesday, April 27, 2016).

[277] Clark Boyd, "Profile: Gary McKinnon," in: ***http://goo.gl/5p6rN7***, (Saturday, April 30, 2016).

ما قام به ماكينون كان قبل 15 سنة، فمما لا شك فيه، أصبحت الآن المعرفة أكثر توفرا وإتاحة من ذي قبل، في إشارة إلى أن المنطق الذي ترمي إليه فكرة الحقول المتداخلة والأداء الوظيفي التعددي في الذهن (Human Multitasking)، أصبحت تمتلك مساحة أكبر فأكبر في ذهنية الفرد، كحقيقة مُحتمة، وكشرط أساسي لمواكبة العصر، وفهم الأحداث التي تجري حاليا في العالم.

أما فيما يخص نظريات العلاقات الدولية، فقد رأينا مختلف الطروحات والتي غلب عليها طابع التأقلم، لكن هذا الأمر لم يمنعها من تقديم بعض الأفكار حيال الأمن الإلكتروني، وإفرازات ثورة المعلومات على العلاقات الدولية فالبنائية حولت إعطاء بعد آخر للرمزية والتحليل القائم على المتغيرات الاجتماعية من أجل فهم ما اصبح يمثله الأمن الإلكتروني، وكذلك محاولة فهم سعي الدول حاليا إلى امتلاك الأسلحة الإلكترونية، عبر التعاطي مع قضايا الأمننة، ودور الخطاب السياسي التي أضافته مدرسة كوبنهاغن. بالإضافة إلى هذا نجد أن الليبرالية هي الأكثر ليونة في التعاطي مع مسالة الأمن الإلكتروني، ولعل ذلك راجع في المقام الأول، إلى أن إفرازات ثورة المعلومات، التي هي نفسها ستوفر الأمن الإلكتروني في ظل اعتماد متبادل أكبر من أي وقت مضى الأمر الذي ضاعف من أهمية القوة الناعمة، وهذا الطرح يعد عكس ما رأته الواقعية التي ترى أن ثورة المعلومات، وبروز الأنترنت، وهواجس الأمن الإلكتروني يعد شيء طبيعيا ومنتظرا متحججتا بأن الأنترنت تمثل النظام الفوضوي الذي طرحته الواقعية بامتياز، ولهذا فإن الواقعية تتعاطى مع المسالة الأمنية ذو البعد الإلكتروني من منطلق وسائلي، إذ تعتبر الأمن الإلكتروني كشق يجب أن يدرج تحت مضلة القضايا التي تتعلق بالقوة العسكرية ووسائل الإكراه ، والدفاع، أو الهجوم؛ فالواقعية إلى جانب النظريات الأخرى ورغم اختلاف منظورها حول الأمن الإلكتروني إلا أن الجميع يتفق على فكرة أن الأمن الإلكتروني، والثورة المعلومات تؤثر بالفعل في الواقع الحالي، بقى أن يحاول كل شخص أن يفهم طبيعة تلك التأثير، وفقا للنظارات التي يلبسها كما قال **والتز**.

كما يجب إضافة أن التعاطي مع مسالة الأمن الإلكتروني، وموضعه من الصراع الدولي، لا يجب التعاطي معه فقط من منطلق هذه النظريات، إذ أن الأمن

الإلكتروني، وبعض النظر على أنه يمثل شعارا جديد لمحاربة الهيمنة، واحد أهم الآليات للقيام بذلك، كذلك من جانب آخر يجب النظر إلى الأمن الإلكتروني على أنه ظاهرة اجتماعية متكاملة، فالأمن الإلكتروني، يمثل طريقة جديدة ومختلفة في التفكير، كما طريقة جديدة في التعاطي مع القضايا، ونحن نتكلم هنا على الطرح المنهجي الذي حاولت مناقشته في السبرانية، والحقول المتداخلة، كما أجيال الحروب أيضا، ومحاولة الذهاب ابعد من ذلك عبر الخوض في موضوع ما بعد الإنسانية، وذلك سعيا إلى توضيح أن الأمن الإلكتروني لا يعبر فقط على آليات وأدوات ميكانيكية، بل يعبر أيضا على عالم متغير على كافة المستويات، عالم متغير يمكننا رؤية ذلك من الآن في ذهنية الأفراد، ومختلف العلماء الذين يبحثون على الأجوبة التي نتعايش معها يوميا.

3.0

نماذج عن الصراع الإلكتروني الدولي

الصراع الإلكتروني، كما النماذج التي يتم مناقشتها، أو أي دراسة لحالة معين لها علاقة بالصراع الإلكتروني تعد جد صعب، كون المخرجات والإفرازات التي تخرج بها في العادة هي مجرد تضارب أفكار، واتهامات بين الدول، خاصة وأن هذه المواضيع تعد معاصرة نوع ما، كما تعد دائما وفي الكثير من الأحيان عرضة للتبويب السياسي، أي ممغنطة معظم هذه الأحداث بالصراع بين روسيا والولايات المتحدة الأمريكية مثلا، أو بين الصين والغرب، أو بين إسرائيل ودول الشرق الأوسط، فمعظم الأحداث الأكثر خطورة تعد مجهولة المصدر، وتهديد مصدرها يكون فقط افتراضيا، وذلك بالاستناد إلى الاتهامات العلنية، كما أن دولة ما مثلا يمكن أن تستند إلى آليات من أجل محاربة هيمنة ونفوذ دولة أخرى، أو العمل على تحقيق النفوذ الخاص، كذلك هي الولايات المتحدة الأمريكية مثلا، فرغم قوتها، إلا أنها تدفع بشدة في الفضاء الإلكتروني لأنه تعرف جيدا، أن الفضاء الإلكتروني يشبه إلى حد بعيد قضية ملأ الفراغ، فبذلك تعمل كل دولة مهما كانت قوتها أو ضعفها على اللعب على هذه الأوتار التي لها علاقة بأقنية الهيمنة الإلكترونية في العالم، كما اللعب على هذه الأقنية من أجل جلب المصالح، والتأثير على اكبر مساحة ممكنة.

في ذروة الحرب الباردة، قام قمر صناعي أمريكي للإنذار المبكر سنة 1982 بالكشف على انفجار هائل في صحراء سيبيريا الشمالية، لكن لم يعرف إذا كان الأمر هو انفجار نووي، أو إطلاق لصاروخ باليستي، لكن تبين فيما بعد أن ذلك المصر الهائل للحرارة التي ألتقطه القمر الصناعي كان سببه انفجار هائل في أنابيب نقل الغاز في الاتحاد السوفييتي؛ فقد كان السبب وراء هذا الانفجار هو عطل في نظام التحكم الحاسوبي للاتحاد السوفييتي الذي تمت سرقته من قبل جواسيس سوفييتيين من أحد الشركات في كندا، لكنهم لم يعلموا أن وكالة المخابرات المركزية الأمريكية قامت بالعبث بتلك الحواسيب والبرمجيات الموجودة فيها عن بعد، ليفقد النظام صوابه بعد مدة معينة، ويتم تغيير سرعة الدفع في أنابيب الغاز الأمر الذي أدى إلى زيادة الضغط في مرحلة ما إلى درجة خارجة عن السيطرة ونتج عن الأمر انفجار هائل، وقد كان الانفجار هائل لدرجة أن الوزير السابق للقوات الجوية الأمريكية **توماس ريد** (Thomas Reed) أكد أن ذلك انفجار كان اعظم انفجار غير نووي رآه في حياته.[278]

يمكن أن نفهم من هنا أن الصراع الإلكتروني والنماذج التي سنتطرق إليها، ستكون في نفس السياق، فآليات المحاربة أو الدفاع، يمكن أن تعبر على عدة أشياء في نفس الوقت، كأن تكون آليات

[278] "War in the fifth domain," in: ***http://goo.gl/N6xi1U***, (Saturday, May 28, 2016).

الدفاع موجهة لإلحاق الضرر عند الهجوم عليها، وليس فقط الدفاع القائم على حماية منطقة معينة، فطبيعة أنظمة المعلومات، تجعل من نفشي الأسلحة الإلكتروني، أو المخاطر التي لها علاقة مباشرة بهذه الأسلحة، أمرا سريعا، ويصعب مجاراته؛ فالذي يمز هذا الصراع الإلكتروني والتجاذب بين محاربة وبسط الهيمنة، هو السرية الكبيرة التي يتميز بها، رغم أن المدخلات الإلكترونية يمكنها أيضا أن تؤثر على الواقع المعايش، وذلك بالتأثير على المرافق التي لها علاقة مباشرة بمصالح المواطنين.

ولهذا سنحاول هنا ذك بعض النماذج كي نوضح هذه الأساليب الجديدة في بسط الهيمنة، كما محاربتها من جانب آخر ومنع اكتساب القوة على دول أخرى، أو جماعات، أو أشخاص، فالصراع الإلكتروني لا يتعلق بالفواعل الرسمي فقط، بل هو كما قلنا سابقا يعبر على دوامة من التفاعلات.

3.1 إستونيا 2007

يعد هجوم تايتن راين (Tian Rain) أو عملاق المطر الذي حدث سنة 2003 أحد أول الهجمات المسجلة في التاريخ والتي تميزت بتنسيق عالي جودة من قبل القراصنة الظين أرادو الدخول إلى العديد من الملقمات، والحواسيب التي كانت تتواجد في الولايات المتحدة الأمريكية، الأمر الذي أدى إلى تسريب، وسرقة العديد من المعلومات، من عدة شركات امنيه، وصناعية.

يعد هذا الهجوم الذي حصل ضد الولايات المتحدة الأمريكية الأول من نوعه، خاصة أنه استهدف قطاعات محددة ومعينة، كما تم استخدام طرق عديدة ومستمرة من اجل الولوج إلى المعلومات المخزنة، فقد اصبح هذا النوع من الهجوم يسمى حاليا بالتهديدات المستمرة المتقدمة (Advanced Persistent Threats - APTs)، ويعبر هذا المفهوم على القراصنة الذين لديهم مصادر كبيرة للمعلومات، كما لديهم قدرات عالية جدا في القيام بعملهم، فعكس باقي القراصنة، تشير كلمة المثابرة هنا (Persistent) إلى الإصرار المستمر والمتعدد الأهداف للقرصان، الأمر الذي يجعل من الصعب جدا إيقاف هذا النوع من الهجمات الذي يمكن أن يستمر لمدة أسابيع.[279]

[279] Net Moran, "Understanding Advanced Persistent Threats," in ***Login***, No 4, Volume 36(August, 2011), pp. 21-26.

لقد كان هجوم العملاق ضد الولايات المتحدة الأمريكية يشير وفق العديد من الخبراء إلى أن المصدر الذي أتى منه الهجوم هو الصين، لكن التأكيد غير موجود في ظل عدم إعلان الحكومة الصينية لذلك (State Sponsored Espionage). وإلى حد الآن لا توجد هناك معلومات حقيقية حول المصدر الحقيقي للهجوم، إذ هذا النوع من الهجوم مثل ما هو الحال مع هجوم حجب الخدمات، يستعمل العديد من الحواسيب المقرصنة حول العالم، يمكن أن تكون الحواسيب الصينية هي أحد تلك الحواسيب المستخدمة أيضا، بالإضافة إلى ذلك فالقطاعات المستهدفة والتي سنراها هنا، توحي بأن ليس الصين وحدها التي يمكنها أن تستفيد من المعلومات التي تم تسريبها؛ فمن بين أهم الشركات التي تم استهدافها، سنجد شركة لوكهيد مارتين (Lockheed Martin)، والغدارة الوطنية للملاحة الجوية والفضاء (National Aeronautics and Space Administration).[280]

لقد قمت بعرض هذا النموذج التمهيدي لأنه يدخل في سياق النموذج الذي سيعرض هنا، كون أن النموذج الخاص بإستونيا، قائمة على نفس التهديدات المتسمرة المتقدمة والذي يعد العملاق أول حالة معروفة، لهذا يجب على الأقل فهم ما تمثله هذه التحديدات من اجل فهم جيد للمثال الإستوني، فالنموذج الإستوني يعد من أبرز الأمثلة التي يتم الاستشهاد بها في القضايا التي تتعلق بالحروب الإلكترونية، خاصة وأن الهجوم الذي تلقته هذه الدولة، دفع بها إلى حدود الانهيار السياسي، والاقتصادي، والاجتماعي.

فالقضية الإستونية بدأت بعد بداية بروز إشكال يخص تمثال يجسد الجندي الساقط (Bronze Soldier of Tallinn)، أو الجندي المجهول الذي يمثل تضحيات الاتحاد السوفييتي الجيش الأحمر في الحرب العالمية الثانية ضد النازية في منطقة إستونيا، لكن جزء من الشعب الإستوني كان يرى في ذلك التمثال تعبيرا على للاحتلال والسيطرة السوفييتية على بلدهم خاصة مع نهاية الحرب العالمية الثانية، وكنتيجة لهذه الاضطرابات والتصعيد، قررت الحكومة الإستونية تغيير مكان التمثال، لكن هذه العملية كان لها رد فعل عكسي خاصة من قبل الطبقة الشعبية التي لها علاقة بالأصول الروسية، والتي كانت لديها مشاعر كبيرة حيال هذه العملية لما كان يمثله ذلك الجندي البرونزي من رمزية، الأمر الذي أدى

[280] Nathan Thornburgh, "Inside the Chinese Hack Attack," in: ***http://goo.gl/OoUalr***, (Sunday, May 29, 2016).

بالعديد من المتظاهرين إلى التصادم مع القوات الحكومية مما أدى إلى قتيل واحد، وإيقاف 1300 شخص، وأكثر من 100 جريح.[281]

ومباشرة بعد قمع المظاهرات، بدأت الهجمات الإلكترونية تطلق ضد دولة إستونية من عدة أماكن في العالم، فلأول مرة في التاريخ تعلن دولة أنها تهاجم، ولكنه ليس عبر استخدام الصواريخ أو المدرعات، فقد قام القراصنة بالاستيلاء على أكثر من مليون حاسوب من 75 دولة مختلفة في العالم من اجل استهداف، مختلف المواقع الحكومية، والاقتصادية، إلى جانب التعاملات البنكية، وملقمات تحليل البيانات، والبنى التحتية للاتصالات الأمر الذي سبب خسائر مالية كبيرة، وهلع لدى المواطنين بسبب عدم قدرتهم على سحب الأموال من البنوك،[282] فقد تم استخدام البوت–نت (BotNet) وذلك من أجل شن أعداد هائلة من هجمات حجب الخدمة (Denial of Service Attack-Dos).

لقد بدأت الهجمات على مختلف ضد مختلف الأهداف التي كانت تستند على الاتصالات بطريقة بسيطة جدا، مثل ما هو الحال مع جمع عناوين الإرسال (IP) والهجوم عليها بطريقة حجب الخدمة، كما تم توزيع العديد من الطرق باللغة الروسية في المنتديات على الشبكة، لتوضيح طريقة المشاركة في هذا الهجوم للأشخاص الذين لديهم إمكانيات اقل، ومعرفة اقل بهذا المجال.[283] فقد استمرت الهجمات التي بدأت في 27 أبريل في الزيادة من قوتها وطرقها المعتمدة، لكن يوم 30 أبريل شكل نقطة تحول في الحرب الإلكترونية القائمة، لأنه في هذا اليوم تم إدخال البوت نت كما قلنا سابقا في المعادلة من أجل الحفاظ على قوة الهجمات، وقد صرح وزير الدفاع آنذاك **جاك أفيسكو** (Jaak Aaviksoo) أن عدد البوتات التي تقوم بالهجوم حاليا على بلاده تقدر على الأقل بأكثر من مليون بوت، كما أن الدول التي انطلقت منها الهجمات عديدة، وقد ذكر منها الفيتنام، والولايات المتحدة الأمريكية، والمملكة المتحدة، ومصر، والبيرو، فالأمر الذي بدا في الأول أن الهجوم إنطلق من 75 دولة فقط، تحول فيما بعد إلى 175 دولة.[284]

---

(281) Rid Thomas, "Cyber War Will Not Take Place," in ***Journal of Strategic Studies***, No 1, Volume 35 (2012), pp. 1-28.

(282) Beidleman Scott W, "Defining and Deterring Cyber War," in ***Military Technology***, No 11, Volume 35(2011) 57-62.

(283) Piter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," in: ***http://goo.gl/w1zGHX***, (Sunday, May 29, 2016).

(284) Michael Phillip Roush, ***Securitization And Desecuritization In Estonia's Cyber Politics***, Master's Thesis, not published (University of South Florida: School of Social Sciences, 2015), p. 45-46.

لقد استمرت الهجمات حتى بعد 17 ماي، ثم قلت حدتها لتزول فيما بعد تمام، لتبدأ العديد من الاتهامات إذ أنه هناك العديد من الأشخاص ومن بينهم الوزير الإستوني الأول، الذي اتهموا روسيا، وذلك أن العديد من الهجمات كانت انطلاقا من ملقمات روسية، لكن الأمر يتعلق مثل العادة بالسؤال الذي يطرح حول إذا أن السلطات الروسية قامت بمباركة هذا الهجوم ودعمه تقنيا، الأمر الذي لم يتمكن أي أحد من إثباته بالأدلة، خاصة بعد أن صرح العديدة من الأشخاص على غرار (Konstantin Goloskokov) الذي اعلن مسؤوليته على هذه الهجمات؛ حتى أن الشركة المتخصصة في الأمن الإلكتروني (F-Secure) صرحت أنه هناك فقط عنوان واحد يمكن تتبعه إلى مصدر حكومي رسمي، ولكن هذا لا يعني شيء، كون أي شخص يمكنه أن يقوم بذلك باستعمال ذلك الحاسوب، كما يمكن أن يكون هو أيضا ضمن البوت–نت (Zombies).[285]

هناك أيضا من يرى أن الهجوم على إستونيا يعد بمثابة إرهاب إلكتروني، أو مجرد احتجاج من طرف قراصنة روسيين، فهذه الحقيقة ممكنة ولا يمكن إنكارها؛ لكن من جانب آخر أيضا لا يمكن إهمال احتمال أن الهجمات كانت مبرمجة بطريقة دقيقة، وبمساندة من جهات رسمية أيضا.[286] يمكن رؤية الاتهامات الجديدة بعد 2007 ضد روسيا في الحرب الجورجية خير مثال على ذلك، إذ انه وأثناء الحرب الجورجية الروسية سنة 2008، تم الهجوم أيضا على مختلف المواقع الحكومية والاقتصادية، إلى درجة أن مجموعة من القراصنة الروس، قاموا بقرصنة مراكز الاتصال لتوفير الخدمات، وقاموا أيضا بفصل جورجيا كليا على الشبكة العنكبوتية العالمية، ولكن مجددا نددت روسيا بالاتهامات الموجهة ضدها، معتبرتا أن ذلك قد أقيم من طرف أشخاص أحرار لديهم تعاطف مع ما نقوم به أو مصالح مادية وراء القيام بذلك.[287]

في الأخير هنا، وبغض النظر عن الجهة المسؤولة عن الهجوم، يمكننا أن نرى الأهمية الكبيرة التي أصبح يتمتع بها الأمن الإلكتروني، كما من جانب آخر الخطورة الكبيرة للحرب الإلكترونية، فإذا كانت هذه الحوادث قد حصلت سنة 2007، فالمؤكد حاليا أن القراصنة لديهم الآن إمكانيات أكبر، وقدرات أوسع لإلحاق الضرر، ولقد قلت قراصنة هنا افتراضا أن الذين قاموا بالهجوم، هم أشخاص وليسوا دول،

---

[285] ***Ibid***, pp. 47-49.
[286] Nicholas C. Rueter, ***op.cit***, pp. 14.
[287] Richard A. Clarke, Robert K. Knake, ***op.cit***, pp. 17-20.

نلاحظ هنا بروزا قويا للفواعل الغير رسمية في العلاقات الدولية، فبغض النظر إذا كانت دولة أو أشخاص، فإن وسائل إلحاق الضرر هذه تعبر فعلا على جيل جديد، وثورة معلوماتية لا زلنا إلى حد الآن نعيش أحداثها.

3.2 ستوكسنت 2010

يعد نموذج ستوكسنت أحد النماذج التي توضح لنا كيف يمكن للحرب الإلكترونية، والأمن الإلكتروني، أن يوكنا في قلب معادلة الصراع في العلاقات الدولية، كيف لا، ولدينا هنا نموذج واضح لكيف يمكن لرموز حاسوبية أن تؤثر على عمل مفاعل نووي، تؤثر عليه بطريقة يمكن أن تدفع لأجهزة الطرد المركزي بزيادة سرعتها أو تقليل سرعتها لتفادي تخصيب اليورانيوم، أو حتى خلق خلل حاسوبي يمكن أن يؤدي بالقضبان التي تساهم في تبخر الماء وتحريك التوربينات(turbines) بالذوبان محدثتا بذلك كارثة إنسانية، وبيئية من اعلى المستويات.

يمكن النظر إلى ستوكسنت (Stuxnet) على أنه نموذج آخر من الصراع الدولي، جيل جديد من الأسلحة، وعصر جديد من الأفكار، وهذا ما يوافق عليه الخبير في الفيروسات الإلكترونية إيريك شان (Eric Chen) والذي يعمل في مخابر سيمانتاك (Symantec) لتحليل المخاطر الإلكترونية المتقدمة، والذي يرى أنه لا يمكن تخيل شيء أكبر من ستوكسنت حاليا، والشيء الوحيد الذي يمكنه أن يقول عليه أنه اكبر من ستوكسنت، هو اختراع الأنترنت نفسها.[288] بدأت معضلة ستوكسنت في جانفي سنة 2010، بعد أن قامت شركة متخصصة في الأمن الإلكتروني في بلاروسيا برصد هذا الفيروس وعزله، كون أن أحد مستخدميها الذين كانوا متواجدين في إيران أعلن بوجود مشاكل في حاسوبه، بعد شهر من هذا الاكتشاف تم توزيع هذا النموذج على العديد من خبراء الأمن الإلكتروني في العالم من أجل معالجته والبحث فيه، الأمر الذي حصل مع **ليام أومـاركو**(Liam O'Murchu) الذي يعمل كمدير تنفيذي لأحد ابرز شركات الأمن الإلكتروني في العالم والتي ذكرناها سابقا وهي (Symantec)، لما

(288) Need to Know WLIW, "Stuxnet Virus," in: ***https://youtu.be/SAy46DhWW8Y***, (Sunday, 29 May 2016).

أقـر بـالجودة العاليـة لهـذا الفيـروس، المكـون مـن مـا يزيـد علـى 18 آلاف سـطر مـن الرمـوز المكتوبـة بكفـاءة عاليـة جـدا، كمـا رأى **أومـــاركو** أيضـا أن مـثلا هـذه الفيروسـات لا يمكـن برمجتهـا مـن قبـل هـواة، ويمكـن معرفـة مـن خـلال طريقـة عملـه أن تصـميمه دام لسـنوات، وأن ذلـك كـان على يد خبراء من عدة مجالات. (289)

فقـد تبـين أن هـذا الفيـروس قـد تمكـن بشـكل سـريع مـن 60.000 ألـف حاسـوب وأن أكثـر مـن نصـف هـذه الحواسـيب كانـت موجـودة فـي إيـران،(290) الأمـر الـذي أكـده **أومـــاركو** أذ يؤكـد أنـه بعـد تحديـد مختلـف الحواسـيب التـي يوجـد بهـا الفيـروس، تبـين أن 70% مـن الحواسـيب المعنيـة بـالأمر موجـودة فـي إيـران، كمـا أن الغريـب فـي ستوكسـنت أنـه كـان يعمـل علـى عكـس بقيـة الـدود الإلكترونـي الـذي كـان يحـاول سـرقة المعلومـات البنكيـة، والأرقـام السـرية، فقـد كانـت لـه أهـداف محـددة لهـا علاقـة خاصـة بالعمليـات الصـناعية والاقتصـادية، وبـالأخص، كـان يبحـث علـى علبـة مميـزة تسـمى بـ (Siemens S7-300)، والتـي يمكـن برمجتهـا للقيـام بوظـائف معينـة، ويمكـن إيجـاد مثـل هـذه العلـب، فـي محطـات الكهربـاء، والمـاء، والنووية، وبرمجة إشارات المرور، ونقل الغاز، والنفط.(291)

كمـا تبـين أن هـذا الفيـروس يواجـه تحـديا خاصـة بعـد أن تبـين أن ستوكسـنت فيـروس جـد معقـد، ولـم يـرى مثـيلا لـه مـن قبـل، وقـد كـان يعمـل فـي البريـة لمـدة طويلـة قبـل أن يكتشـف، كمـا أنـه تبـين أنـه ينتقـل فقـط عبـر اسـتخدام ذاكـرة البيانـات(flash drive)، ولـيس الأنترنـت، الأمـر الـذي كـان يعنـي أنـه يجـب زرعـه فـي منـاطق محـددة بطريقـة يدويـة، لعـل هـذا الأمـر، أي جعلـه لا ينتقـل عبـر الأنترنـت كـان لأسـباب تتعلـق بتقفـي الآثـار، فالفيروسـات تعمـل بطريقـة أحسـن لمـا تكـون فـي أنظمـة مغلقـة، ونحـن نـتكلم هنـا خاصـة علـى هـذا النـوع مـن الفيروسـات التـي تسـتهدف الهياكـل الحيوية للدولة، والتي يستوجب التأثير عليها قدرا عاليا جدا من السرية.(292)

(289) MMXII CO5 Interactive, "Stuxnet: Computer worm opens new era of warfare," Documentary in: ***https://youtu.be/6WmaZYJwJnq***, (Sunday, May 29, 2016).
(290) Farwell James P, Rafal Rohozinski, "Stuxnet and the Future of Cyber War," in ***Survival***, No 1, Volume 53(2011), pp. 23-40.
(291) MMXII CO5 Interactive, ***op.cit.***
(292) Anthony F. Sinopoli, ***Cyberwar and International Law: An English School Perspective***, Master's Thesis, not published (University of South Florida: Scholar Commons Citation, 2012), p. 41.

الصورة رقم: 3.0

صورة توضيحية لجهاز (Siemens S7-300)؛ حجمه حوالي 15*15سم. [293]

بعد القيام بالهندسة العكسية(Reverse Engineering) لستوكسنت تبين أنه هذا الفيروس موجه ضد أهداف جد محددة ودقيقة، فبعد العلبة التي ذكرناها سابقا، تبين أن الفيروس يبحث أيضا على نشر العدوى في العديد من المعدات التي لا يمكن إيجادها إلى في المحطات النووية، والتي يمكنها أن تؤثر بشكل مباشر على سرعة أجهزة الطرد في المفاعلات النووية، كما تخريب العديد من أجهزة، وأنظمة الطرد المركزي (Nuclear Centrifuges) في المفاعل النووي الإيراني المتواجد في نطنز (Natanz)، وذلك عبر استعمال سلسلة من الرموز المشفرة.

فبعد أن تمكن **أومـاركو** سنة 2012 إلى جانب العديد من الخبراء من فهم ستوكسنت جيدا، كان الفيروس قد حقق جزء من الأهداف التي كان يريدها مصنعوه، فشهر قبل أول اكتشاف للفيروس سنة 2010 قام خبراء، ومراقبين من الوكالة الدولية للطاقة الذرية (International Atomic Energy Agency) برفع تقارير تتكلم على أن الجانب الإيراني يعاني العديد من المشاكل المتعلقة بأجهزة الطرد المركزي في مفاعل نطنز، كما تكلمت تقارير أخرى أيضا على أن الجانب الإيراني قام باستبدال 2000 جهاز للطرد المركزي لأسباب

(293) "Image of the Siemens S7-300," in ***http://qoo.gl/lB6zmp***,(dimanche 29 mai 2016).

مجهولة؛ فالذي صمم ستوكسنت يعرف جيدا كيف تعمل المفاعلات النووية إلى ابعد حد، كما كانوا على دراية جيدة، بالنموذج التي تستخدمه إيران من أجل تخصيب، أو استغلال الطاقة الذرية.[294] وهناك حتى من يؤكد الضرر ويقول أن من بين 2000 جهاز الذي نزع، 1000 جهاز كانت سببه فيروس ستوكسنت.[295]

رغم العديد من التقارير، والاتهامات التي تشير إلى أن ستوكسنت هو شراكة إسرائيلية–أمريكية، إلا أن عدم قدرة أي جهة على معرفة الحاسوب الأول المصاب (Patient Zero)، كما أن المواقع التي كانت تتلقى المعلومات التي يجمعها الفيروس تم فتحها عبر استخدام بطاقات بنكية مسروقة، جعلت من معرفة الأصل شيء مستحيل بدون أدلة قاطعة؛ لكن من جانب آخر هناك العديد من الأسئلة المهمة التي يجب طرحها هنا، وهو الأمر الذي قام به غاري براون (Gary Brown)، لما تساءل عن سبب عدم إعلان إيران أنها هوجمت، وأنها تلقت هذه الأضرار، لكن يبدوا أن الإجابة تكمن في أن إيران ليس من مصلحتها القيام بإعلان علني عن هذا الهجوم، خاصة وأنها كانت في وضح مميز حيال مشروعها النووي، وموضوع الرقابة الدولية، فإيران تعرف حاليا، وبطريقة جيدة أن الحرب الإلكترونية قد أعلنت منذ مدة وعليها أن تتأقلم مع قواعد اللعبة الجديدة.[296]

استخدام الأسلحة التقليدية ضد هدف معين، يؤدي إلى تدمير الهدف، والسلاح الذي أستخدم أيضا (صواريخ، رصاص ...)، عكس الأسلحة الإلكترونية التي لا تُستهلك أو تُدمر عند القيام بالعمليات، فستوكسنت غير فعلا نظرة الدول إلى الحروب الإلكترونية، وغير أيضا نظرة الدول إلى امنها الإلكتروني، فهذا الفيروس لا يعد الأخير، ويمكننا رؤية ذلك في بروز ما يسمى بفيروس فلايم (Flame) الغير مدمر، والذي يهدف أكثر إلى التجسس وجمع المعلومات، ولكن الأخطر من ذلك حاليا، وبسبب الهندسة العكسية، يمكن لأي جهة حاليا أن يحمل فيروس ستوكسنت ويستغله لأغراضه الخاصة، أي شخص مهما كان يمكنه دخول الشبكة العنكبوتية وتحميل كود اصل هذا الدود، فإطلاق سلاح إلكتروني في البرية يعد أكثر خطورة من استخدامه، إذ أن العدو يمكنه أيضا رصد الفيروس، ثم التعديل عليه واستخدامه

---

(294) MMXII CO5 Interactive, ***op.cit.***

(295) Anthony F. Sinpoli, ***op.cit***, p. 42.

(296) Gary D. Brown, "Joint Force Quarterly," in ***JFQ Marine Corps***, issue 63, 4th quarter(October, 2011), p. 70-73.

لأغراضه الخاصة، أو ضد مصدر التهديد، يمكننا هن أن نقول أن هذا الأمر يمكن مقارنته بالأسلحة المفتوحة المصدر، أين يمكن لأي شخص أن يستخدمها، أسلحة يمكنها أن تدفع دول بكاملها إلى حدود الانهيار.

في نهاية هذا الجزء من الدراسة نكون قد كوننا نظرة على الصراعات الإلكترونية التي يمكن أن تحدث في العلاقات الدولية، كما مميزات هذا الصراع القائم ومختلف الوسائل التي يتم استخدامها من اجل الدفاع على المصالح، أو محاولة إلحاق الضرر على الجانب الآخر. فهذه إشارة واضحة على كيف أصبحت الدولة تعتمد بشكل أكثر على المعلومات، كما أن الأهداف ليست بالضرورة عسكرية.[297] بالإضافة إلى هذا يجدر معرفة أن هذه النماذج لا تعبر على مختلف إفرازات الثورة المعلوماتية، والتي يمكن النظر إليها على أنها دوامة فعلية من التفاعلات والتضاربات المختلفة، بين مختلف الفواعل الرسمية والغير رسمية، كما أن عدم وجود قضايا تتعلق بالصراع الإلكتروني لا تعني بالضرورة عدم وجودها، ففي هذا المجال، الجميع يعرف أن الإعلان السياسي، عن المواقف لن يغير شيء، إلا إذا ترتب على ذلك سياسات معينة تتعلق بعمل الدولة، ففي قضية العملاق، إلى جانب العديد من الهجمات التي قام بها القراصنة، العديد من الدول كانت تعرف جيدا أنها تعرضت إلى الهجوم، ولكنها لم تكتشف ذلك، بالإضافة إلى هذا لا أحد يمكنه أن يعرف بالتأكيد إذا كان الهجوم من طرف جماعة أو دولة، يمكننا أن نرى هنا أن الثورة المعلوماتية عقدة الأوضاع بطريقة غير مسبوقة، ولا مثيل لها في التاريخ القديم.

نرى هنا بكل بساطة بعض الأمور الواضحة جدا، أولا؛ تعدد الفواعل واتساعها إلى ابعد مستوى يمكن تصوره في العلاقات الدولية، ثانيا؛ تعدد الفواعل عبر بشكل متوازي أيضا على تعدد وسائل الإكراه التي أصبحت متاحة للأشخاص، ثالثا؛ الأمن الإلكتروني أصبح ضرورة لا يمكن المقامرة عليها، رابعا؛ زئبقية القوة، ولامركزيتها، خامسا؛ الرجوع إلى الموسوعية بعد التخصص، سادسا؛ أشكال جديدة من الحروب، من الأنساق الاجتماعية، من طرق التفكير.

---

[297] Jhon Bylis, Steve Smith, Patricia Owens, **The globalization of World Politics** (The United States of America, Published by Oxford University Press, 2014), p.217.

خاتمة

يمثل موضوع الأمن الإلكتروني، بالإضافة إلى مختلف إفرازات الثورة المعلوماتية، أحد أهم المواضيع التي يجب التعاطي معها من أجل فهم جزء من الظاهرة السياسية الحالية، إلى جانب العديد من الظواهر الأخرى، والتي يمكن أن تمتد من الظواهر الاجتماعية إلى القضايا الاقتصادية، والعسكرية، والتربوية، إلى ما هو أوسع. فإن التعامل مع مختلف هذه المجالات، والقطاعات المتعددة، يعود بشكل أساسي إلى ما يعبر إليه الأمن الإلكتروني، فالتعاطي من الأمن الإلكتروني يجب أن يكون موازاتا مع حقيقة أن العالم الحالي أصبح عالما رقميا بامتياز، عالم افتراضي، أين أصبحت معظم التفاعلات الاجتماعية موجودة هناك، لهذا فإن التكلم على الأمن الإلكتروني لا يتعلق فقط بالجانب الأمني الذي يمكن تصوره، فقد عمل الأمن الإنساني على توسيع مفهوم الأمن وعرضه بطريقة لا تتعلق فقط بالجانب العسكري البحت، فثورة المعلومات ورقمنة الحياة الإنسانية على مختلف المستويات، جعلت النظرة إلى مثل هذه المواضيع تعد موسوعية أكثر منها تخصصية، ذلك أن مفاهيم القوة، والأمان تغيرت بشكل كبير، كما أن القاعدة التي يستند عليها الأمن الإلكتروني هي قاعدة متعددة جدا، الأمر الذي جعل من فهم أو الخوض في الموضوع يتطلب اختبار بعض هذه الأجزاء التي يقوم عليها، من اجل معرفة مدى ارتدادات هذه التفاعلات على أرض الواقع، ومدى خطورتها مقارنة مع الوسائل التقليدية للإكراه، أو ما كان يعبر عليه الأمن أو حتى الهيمنة.

رغم أنه لازال ولحد الآن ينظر إلى الأمن الإلكتروني على أنه أثار أكثر منه مفهوما جديد، إلا أن التطرق إلى هذا الموضوع من قبل منظري العلاقات الدولية بدا واضح أنه في تزايد مستمر، كما أن التعامل مع المصطلح أصبح أكثر دقة، ذلك أن الأمن الإلكتروني أصبح يعبر على شيء أكبر من مجرد أشكال أمنية غير أساسية، أو آثار مباشرة للثورة المعلوماتية؛ فالأمن السبراني اصبح يعبر على العديد من القضايا التي تعطينا نظرة حول عالم المستقبل، فبغض النظر على التأثيرات التي يمكن أن نراها اليوم، مثل ما هو حال مع بروز ما يسمى بالأسلحة الإلكترونية في الخطابات السياسية لقادة العالم، أو الحرب الإلكترونية، يعبر الأمن الإلكتروني أيضا في المقابل على مواضيع أعمق، إذ أنه يمكننا اليوم رؤية أننا في تحول إلى جديد، عالم توجد بع قواعد جديدة ومفاهيم جديدة فرضت نفسها على الجميع، أو بالأخرى على كل من يريد أن يلحق بركب التطور الإنساني، يمكننا أن نرى اليوم العديد من القضايا التي تتعلق بالخلايا الجذعية التي ترمي إلى خلق أعضاء جديدة، يمكننا أن نرى اليوم بداية بروز حواسيب كمية ستدفع حدود التصميم والبحث البشري إلى نقطة ابعد، يمكننا أن نرى اليوم أيضا بروز تكنولوجيات الوصل العصبي مع الهياكل الميكانيكية، مثل هذه القضايا إلى جانب العديد من التكنولوجيات الصاعدة تبين لنا أن القاعدة الرقمية أثبتت وجودها حاليا، والمرجح أن ذلك سيكون لمدة طويلة؛ ومن جانب آخر

توضح لنا أيضا دفع الحدود البشرية إلى اقصى حد مثل ما هو الحال مع طرح البعد إنساني، والذي يمكن رؤيته هنا، إن معظم هذه المبادرات الثورية لها علاقة وطيدة بثورة المعلومات، والأمن الإلكتروني هو بمثابة الحارس الوحيد في هذا العالم التقني المتواجد بشكل أكبر. لكن الفكرة الأهم هنا، هو معرفة أن الصراعات الحالية، والصراعات المستقبلية، ستتخذ شكلا جديدا، وطابعا آخر، في ظل هذه التحولات التي تفرض نفسها يوما بعد يوم، حقيقة أن التقدم التقني سيستثمر عسكريا، ولأغراض السيطرة على الآخر، شيء متوقع والتاريخ خير دليل على ذلك، لهذا سأقول أن دور الأمن الإلكتروني يكمن في النظرة الجديدة للتفكير حول النزاعات، والصراعات، والإكراه، وتامين الذات، كما يشير أيضا إلى تعدد للفواعل، وطريقة إلحاق الضرر.

فأي جيل تقني واضح المعالج، يوضح الإمكانيات التي يمكن الاستناد عليها من أجل إلحاق الضرر والهيمنة على الآخر، كما يوضح أيضا الإجراءات والإمكانيات التي يجب السيطرة عليها من أجل صد هذا النوع من السلوك العدائي، فطبيعة الأمن الإلكتروني، كما الهياكل التي يقوم عليها، إلى جانب اللغة المميزة التي يتميز بها الأمن الإلكتروني، جعل من مهمة مكافحة الصراع قضية يتشارك فيها الجميع، ذلك أن الأسلحة الإلكترونية، وقضايا الاختراق، والقرصنة، تعد بمثابة الأسلحة الموزعة التي يمكن لأي شخص أن يعتمدها من اجل أهداف معينة، مثل هذا الأمور سمحت ببروز المجتمع الإلكتروني كقوة جديدة بارزة ضد الفواعل التقليدية التي كانت تسيطر على القوة، كما سمحت ببروز جيل جديد من أشكال الصراع، يتناقض تمام مع ما جاء به اتفاق وستفاليا. ومن جانب آخر نجد أن الدراسات الأمنية والتي تطرقت إلى بعض مظاهر الأمن الإلكتروني، والإفرازات التي جاءت بها الثورة المعلوماتية، تؤكد على تأثير ثوره المعلومات هذه على المعادلة، ولكن في المقابل، ينظر إلى الأمن الإلكتروني، وما يمثله بطريقة مختلفة، فقد رأينا كيف حاول الطرح الواعي أن يعلب الأمن الإلكتروني بطريقة تجعله أحد الوسائل العسكرية، وأن معالجته يجب أن تستند على ذلك الأساس، خاصة أنه أكد على أن العديد من إفرازات الثورة المعلوماتية، قدمت إلى الواجهة العديد من طروحات الواقعية مثل الفوضى الدولية، بالإضافة إلى هذا نجد نفس السياق في التأقلم مع النظرية الليبرالية التي رأت أن الأمن الإلكتروني يمكن فهمه في مدلول الثورة المعلوماتية التي ستدفع إلى التشابك أكثر في العلاقات بين الدول الأمر الذي سيسمح بزيادة فرصة السلام في العالم؛ سنرى هنا أن النظريات تعاملت مع مفهوم الأمن الإلكتروني بطريقة حذرة جدا،

الأمر الذي يوحي أن التفاعلات الدولية التي تستند على قضايا الأمن، والثورة المعلوماتية يجب أن تكون أكثر إلحاحا من أجل رؤية الأمن الإلكتروني كمتغير مستقل ومهم من أجل فهم العلاقات الدولية.

يمكننا أن نرى من هنا كيف استطاع الأمن الإلكتروني أن يخلق نقاشا في العديد من مجالات الحياة الإنسانية، فكل ما هو مرقمنا يدخل في نطاق الأمن الإلكتروني، فهذا التشابك الذي جاء به، ويمثله الأمن الإلكتروني، يستحق، بل يجب أن يدرس بطريقة مختلفة على الدراسات الأمنية السائدة، فالتداخل الكبير في التخصصات التي يمكن أن يستند عليها الأمن الإلكتروني، كما التأثيرات التي يمكن أن يسببها أيضا، جعل من محاولة فهم هذه الظاهرة الجديدة عملية يجب التعمق فيها، والمشاركة فيها من قبل عدة تخصصات وخبراء، من أجل فهم فحوي الأمر، ولهذا ينظر إلى ثورة المعلومات على أنها العودة الجديدة إلى الموسوعية؛ الحقائق تفرض على الباحث حاليا أن يذهب أبعد من أجل فهم الظواهر السياسة التي تحدث، كما من أجل فهم الأنماط، والأنساق التي يقوم عليها الصراع حاليا، والتي من الممكن تتبعها، وفهمها إذا نظرنا للموضوع بصورة اكبر.

لقد خرجت بمجموعة من النقاط والتوصيات المهمة التي يمكنها أن تعبر على الموضوع بطريقة مفتاحية، ويمكن عرض هذه النقاط وفقا لما يلي:

1. يعبر الأمن الإلكتروني بعمقه الحالي على ظاهرة جديدة قامت بهندستها ثورة المعلومات ودراسات السيبرنطيقا، كما يعبر أيضا على طريقة جديدة، ومختلفة في النظر إلى الأحداث الإنسانية وتفسيرها، ويجسد نمطا جديدا للتقدير الذهني الذي يجب علي أي باحث أن يتعلمه، ويفهمه، من أجل إدراك، وفهم المتطلبات التي تفرضها بعض القضايا مثل الهيمنة، والحروب، والصراعات، ففهم الأمن الإلكتروني يشير في المقابل إلى اكتساب القدرة على تحسس ما تحت الأرض، وفهم أعمق لحقيقة أن الأمن الإلكتروني يشير إلى نهج جديد في التعاطي مع العالم، كما يشير ويعبر أيضا على جزء من مُحصلة ثورة المعلومات، والتفاعلات الإنسانية المختلفة.
2. لا يجب النظر إلى الأمن الإلكتروني على أنه مفهوم يخالف الطرح التقليدي للأمن، أو الطرح الذي جاء به الأمن الإنساني، يمكن رؤية الأمر على أنه هناك حقيقة، وهذه الحقيقة تقول أنه هناك حاليا عالم إلكتروني، عالم فتراضي موازي، عالم أصبح بمثابة الامتداد الرقمي للعالم الحقيقي الذي نعيش فيه، هذا العالم قام بمحاكات وجسد معظم متطلبات الحياة الإنسانية التي كان يعيشها، بداية من ابسط الأمور مثل الشراء، والتبضع، والتعلم، مرورا بمواضيع اكبر قليلا مثل الاستثمار، والتبادلات

التجارية، إلى قضايا نزاعية شاملة، مثل الصراع، والهيمنة، والتدمير، وإلحاق الضرر المادي والمعنوي.

3. إذا أردنا تقديم مفهوم شامل للأمن، فهذا يعني في المقابل، تقديم مفهوم شامل لكل شيء، هذه الفكرة تشير إلى مدى تشعب التقنيات في الحياة الإنسانية، فبغض النظر على التأثيرات الفيزيائية التي جاء بها الأمن الإلكتروني على مختلف مصادر، أو هياكل الحياة الإنسانية، إلا أن الشيء الآخر المهم هنا، هو التقدير الإنساني، وبالأخص التقدير الذهني، فالأمن الإلكتروني، وثورة المعلومات خلقت مجموعة من التيارات الفكرية الواضحة، مجموعة من الثقافات، وطرق التفكير التي تميز العصر الحالي، والتي ستؤثر بشكل واصح على طريقة رؤية الناس للعالم الخارجية، وكيفية التفاعل مع الطرف الآخر، إلى جانب كيفية العيش، وكيفية ممارسة الحرب، والتعليم، والهيمنة، أي كيفية العيش بصفة عامة، مثل هذه الأفكار تشكل الوعي العالمي الحالي، ولها اثر كبير في تحديد معالم عالم المستقبل.

4. الذي لا شك فيه، هو أن الأمن الإلكتروني يناقش موضوع الحرب الصراع بطريقة عميقة، خاصة إذا ما تعلق الأمر بحروب الجيل الخامس كما وضحت سابقا، كما يوضح لنا أيضا الآليات التي أصبحت تستخدم من أجل الدفاع أو الهجوم في ظل هذا الجيل الجديد من الصراعات والسباق نحو التسلح، كما يوضح لنا أيضا بروز مجتمع إلكتروني أصبح معنيا بهذه الصراعات، أكثر من الدول نفسها في بعض الأحيان، والذي أصبح يشكل تهديدات كبيرا للأمن القومي للدول، بسبب هامش الخسائر السياسية، والإقتصادية، والإجتماعية المحتملة، فرغم أن الحرب الإلكترونية لا يمكنها أن تشكل الحسم في أي حرب حالية، إلا أن ذلك سيتغير في قريبا في ظل الاعتماد أكثر على الذكاء الاصطناعي في الحروب.

5. شكل الأمن الإلكتروني تحديا نظريا جديدا في حقل الدراسات الأمنية، فلو أسقطناه على طرح ناي، فالأمن الإلكتروني مثل الحب، أي أن الشخص، يعد غارقا في عالم تحكمه التكنولوجيا على مختلف مستوياته الحيوية، والقاعدية، لكنه يجهل تماما طريقة سير هذا العالم. ولهذا يمكنا أن نرى قريبا اهتمام أكبر بالأمن الإلكتروني كمتغير مستقل عن الثورة المعلوماتية، والحقيقة هنا، إنني أرى أن هذه الثورة الجديدة، والزحم الكبير الذي جسده الأمن الإلكتروني، قد تعدى قليلا طروحات مختلف النظريات التي تنظر في حقل الدراسات الأمنية، فالقوانين الدولية مثلا، وبالأخص منظمات الإغاثة الإنسانية، وحقوق الضحايا، تشير على أنه يجب أن يكون هناك تحيين مستمر للقوانين، كي لا يتم تجاوزها من قبل التطور التقني، لكن كما راينا فيما يخص قوانين أيزو، ميزة الأمن الإلكتروني، أنه

يمثل عالم يتطور بشكل مستمر، يمثل أسلحة في تطور يومي، ووسائل يومية وجديدة في إلحاق الضرر، بالإضافة إلى تشابك تام، ومتعدد، ومعقد مع مجالات متداخلة، لها علاقة سببية أو وظيفية، لهذا يمكن أن نفهم أن النظريات التي تكلمت على الأمن، عالجت هذه الظاهرة الجديدة من منطلق عناوين عامة، في انتظار تحدد معالم هذا العالم الجديد، ورؤية ما يمثله الأمن الإلكتروني فعلا في المعادلة الدولية.

6. بروز أهمية كبيرة للدراسات المتداخلة، والتي أصبح تعبر على الطريقة الجديدة في التعاطي مع القضايا، والمواضيع السياسية، فقد رأينا العديد من المحاولات التي جمعت مجموعة كبيرة من مختلف التخصصات، وذلك من اجل فهم، أو الإجابة على الأسئلة التي هي قيد المعالجة، فقد ساهمت الثورة المعلوماتية في تجسيد اكبر لهذا الطرح في القرن الحالي والماضي، فالقضايا والمشاكل، أصبحت أعقد، واكبر من أن تحل من حقل دراسي واحد، ففهم الظاهرة الأمنية حاليا لا يمكن فهمها فقط عبر التعاطي معها من منطلق سياسي نظري، إذ على الباحث حاليا أن يعرف ما هو **ممكن**، وما هو ممكن هنا يعبر على معرفة حدود الإمكانيات الممكنة للتكنولوجيات الحالية، وهذا الأمر لا يمكن تحقيقه، إلى عبر النظر وتحليل القضايا بصورة مختلف وأشمل، وتلك الشمولية طبعا يتم اكتسابها، عبر المعالجة الشخصية المتعددة، أو عبر التشارك في معالجة القضايا أو الأسئلة المطروحة. ومن جانب آخر، فالتداخل التخصصي، لا يعد بالضرورة آلية يجب الاعتماد عليها، لكن ذلك يبقى رهينة اختيار الباحث، ونظرته لموضوع البحث؛ والتي أرى شخصيا أن موضوع الأمن الإلكتروني لا يمكن مناقشته ومعالجته فعليا بدون التطرق إلى حقول نظرية وعلمية أخرى.

“One must always aim for the moon, for if one fails, one will always fall among the stars”.

~ Oscar Wilde

5.0

قائمة المصادر والمراجع

المراجع باللغة العربية:

الكتب:

0. ذياب، البداية. ***الأمن وحرب المعلومات***. عمان: نشر من طرف دار الشروق للنشر والتوزيع، الطبعة الأولى، 2006.
1. ريتشارد، كلارك وروبرت، نيك. ***حماية الفضاء الإلكتروني في مجلس التعاون الخليجي***. أبو ظبي: نشر من طرف المركز الإماراتي للدراسات والبحوث الإستراتيجية، الطبعة الأولى، 2011.
2. سامي، عياد. ***استخدام تكنولوجيا المعلومات في مكافحة الإرهاب***. مصر: الإسكندرية، نشر من قبل دار الفكر الجامعي، الطبعة الأولى، 2007.
3. صفات، سلامة. ***أسلحة حروب المستقبل بين الخيال والواقع***. أبو ظبي: نشر من قبل المركز الإماراتي للدراسات والبحوث الإستراتيجية، الطبعة الأولى، 2005.
4. الغثير، خالد بن سليمان والقحطاني، محمد بن عبد الله. ***أمن المعلومات***. السعودية: جامعة الملك سعود، نشر من قبل مركز التميز للأمن المعلوماتي، الطبعة الأولى، 2005.
5. مصباح، عامر. ***نظرية العلاقات الدولية***. مصر: القاهرة، نشر من قبل دار الكتاب الحديث، 2009.
6. البشري، محمد أمين. ***التحقيق في الجرائم المستحدثة***. الرياض: نشر من قبل جامعة نايف للعلوم التكنولوجية، الطبعة الأولى، 2004.

المذكرات:

0. سعيد جلعود، وليد غسان. ***دور الحرب الإلكترونية في الصراع العربي الإسرائيلي***، مذكرة ماستر، غير منشورة، فلسطين، جامعة النجاح الوطنية: كلية الدراسات العليا، 2013.
1. ساعو، وليدة. ***الثورات العربية بين التوازنات والتفاعلات الجيوستراتيجية ومتغيرات المنقطة العربية***، مذكرة الماستر، غير منشورة، الجزائر، بسكرة، جامعة محمد خيضر: كلية الحقوق والعلوم السياسية، 2013.

المقالات:

0. بشارة، عزمي. "عن المثقف والثورة،" تبين، العدد 4 (ربيع، 2013)، ص ص. 128- 142.
1. بوكنان، مارك. "التداول بسرعة الضوء،" الطبيعة، العدد 31(إبريل، 2015)، ص ص. 39-41.
2. تشارلز، إي لايسرسون وتشاك، ماكفيني. "يحتاج أساتذة العلوم إلى تدريب على مهارات القيادة،" الطبيعة، العدد 36 (سبتمبر،2015)، ص ص . 39-41.
3. زاسترو، مارك. "كوريا الجنوبية: الجامعة المقلوبة،" الطبيعة، العدد 27 (ديسمبر، 2014)، ص ص. 39-40.
4. سافاج، نيل. "بناء الفرص،" الطبيعة، العدد 22 (يوليو، 2014)، ص ص. 93-94.
5. ليدفورد، هايدي. "التخصصات المتداخلة: لماذا يجب على العلماء أن يعملوا مع لإنقاذ العالم،" الطبيعة، العدد 38 (نوفمبر، 2015)، ص ص. 93-94.
6. والدروب، ميتشيل. "ما بعد قانون مور،" الطبيعة، العدد 44 (أبريل، 2016)، ص ص. 32-35.
7. الجهيني، دعاء. "الأحلاف الإلكترونية،" اتجاهات الأحداث، العدد 6 (يناير، 2015)، ص ص. 11-13.

المواقع الإلكترونية:

0. خريطة تناسبية (Treemap) تمثل الدول الرائدة في مجال الحواسيب الفائقة القدرة، في: ***.http://www.top500.org/statistics***

الأشرطة المصورة:

0. جون ميرشايمر، الواقعية البنيوية، شريط مصور، في: https://y***outu.be/gh6bYUsJY6g***، الثلاثاء، 12 تموز، 2016.

<u>المراجع باللغة الفرنسية</u>:

الكتب:

0. Anger, Véronique. ***Sure Les Trace du Groupe des dix***. France : publier par le Forum Changer d'Ère - Forumchangerdere.com, 2013.

المقالات:

0. Jean-Paul Delahaye. "Le Bitcoin, première crypto-monnaie," dans ***Bulletin de la société informatique de France***, No 4 (Octobre, 2014), pp. 67-104.

الأشرطة المصورة:

0. Ivan Macaux, le Turbo Capitalisme, Nouveaux Loups de WallStreet, Documentaire, dans : ***https://youtu.be/vOzH7Aj2MOA***, (samedi 7 mai 2016).

المراجع باللغة الإنجليزية:

الكتب:

0. Sarwono Sutiko. ***Transforming Security Using COBIT®5***.The united States of America, Illinois, published by The Information Systems Audit and Control Association, the first edition, 2013.
1. Abraham H. Maslow. ***Motivation and Personality***.The United States of America: Cambridge, published by Harper & Row, the third edition, 1954.
2. Alan Cole, Philip Drew, Rob McLaughlin. **Handbook on Rules of Engagements**. Italy, Sanremo, published by The International Institute of Humanitarian Law, 2009.
3. Alexander Kott, Cliff Wang, Robert Erbacher. **Cyber Defense and Situational Awareness, Series: Advances in Information Security**. Switzerland: Published by Springer International Publishing, Volume 62, 2014.
4. Amnon H. Eden, James H. Moor, Johnny H. Soraker, Eric Steinheart : **Singularity Hypotheses, a Scientific and Philosophical Assessment**.United Kingdom, Clochester, the School of computer Science, published by Springer Verlag Berlin Heidelberg – Dordrecht London, 2012.
5. Andress Jason, Winterfeld Steve .**Cyber Warfare: Techniques, Tactics and Tools for Security Practitioner** .Online: published by Syngress, the 2nd edition, 2013.
6. Ann Ruth Willner. ***The Spellbinders, Charismatic Political Leadership***.The United States of American: Connecticut, published by Yale University Press, the first edition, 1984.
7. Arturo, Rosenblueth. Norbert, Wiener. Julian, Bigelow. **Behavior, Purpose and Teleology**. The United States of America: published by Philosophy of science association, 1943.
8. Barry Buzan. ***People State And Fear , An Agenda For International Security Studies In The Post-Cold War***.The United States of America, Bonlder published by Lynne Rienner Publishers ,the first edition, 1991.

9. Barry Buzan , Lene Hansen. **The evolution of International Security Studies**. The United States of America: New York, published by Cambridge University Press, the first edition, 2009.
10. Brian Nichiporuk. " U.S Military Opportunities Warfare Concepts of Operation", in **United States Air and Space Power in the 21st Century**, edited by Zalmay Khalizad, Jeremy Shpiro, The United States of America, published by RAND, 2002.
11. Bruce Schneider. ***Secret and Lies، Digital Security in a Networked World***. The United States of America: New York، published by Wiley Publishing, the first edition، 2000.
12. Bruce Schneider. Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code. The Unites States of America: Ney York, published by Wiley Computer Publishing, John Wiley & Sons, Inc, 1996.
13. Bruce Schneider. ***Data And Goliath, The Hidden battle to Collect Your Data and Control Your World***.The United States of America: Ney York, published by W. W. Norton & Company, the first edition, 2015.
14. Carence W. de Silva. ***Mechatronics, a Foundation Course***.The Unites States of America, New York, published by Taylor & Francis Group, the first edition, 2010.
15. Chris C. Demchak. ***Wars of Disurpation and Resilience*** .Athen: published by The University of Georgia, the first edition, 2011.
16. Chris, Dibona. Sam, Ockman. Mark, Stone. Open source. **Voice From the Open Source revolution**.The United States of America, California, published by O'Reilly & Associates Inc, the first edition ,1999.
17. Christopher P.M Water. ***British and Canadian Perspectives on international Law*** .The Netherlands: Leiden, published by Martinus Nijhoff, the first edition, 2006.
18. Colin Wight. "Philosophy of Social Science and International Relations," in ***Handbook of International Relations***. edited by. Walter Carlsnaes, Thomas Risse, Beth A. Simmons .United Kingdom: London, published by SAGE Publication, the first edition, 2002.
19. Daniel Stephen, Halacy. ***Cyborg, the Evolution of the Superman***. The United States of America: New York, published by Harper & Row, the first edition, 1965.
20. Daniel Ventre. ***Chinese Cybersecurity and Defense.*** The United States of America: Hobken, Published by Joan Wiley & Sons Inc, the first edition, 2014.
21. David A, Mindell. Jérôme, Segal. Slava, Gerovitch. Fro**m Communications Engineering to Communications Science, Cybernetics and Information**

Theory in the United States, France, and the Soviet Union, in Science and Ideology: A Comparative History. United Kingdom: London, published by ed. Mark Walker, Routledge, the first edition, 2003.

22. David Bollier. ***The rise of Netpolitik: How The Internet Is Changing Politics and Diplomacy***. The Unites States of America: Washington D.C, published by The Aspen Institute, 2003.
23. Denis McQuail. ***Communication Theory***. The United States of America: California, published by Saga Publication Inc, the first edition, 1983.
24. Edward, Lucas. ***CyberPhobia, Identity Trust Security and Internet***. United Kingdom: London, Published by Bloomsbury publishing, the First edition, 2015.
25. Horach Greeley, Leon Case, Edward Howland, John B. Gough, Philip Ripley, F. B. Perkins, J. B. Lyman, Albert Brisbane, Rey. E. E. Hall, and others. **The Great Industries Of The Unites States**. The United States of America: published by Hartford, 1872.
26. Isaac Asimov. ***Robots and Empire***. The United States of America: Ney York, published by Doubleday, the first edition, 1985.
27. Isaac Asimov ***Runaround, in I, Robot Collections***. The United States of America, New York, published by Street and Smith Publications, Inc, the first edition, 1942.
28. James Bartlet, ***The Dark Net***, ***Inside the Digital Underworld***. United Kingdom: London, published by William Heinemann, the first edition, 2014.
29. Jhon Arquilla, David Ronfeldt. **In Athena's Camp, Preparing for Conflict in Information Age**. The United States of America: Washington D.C, Published by Rand, the first edition, 1997.
30. Jhon Bylis, Steve Smith, Patricia Owens. **The globalization of World Politics. The United States of America**. United Kingdom: Published by Oxford University Press, 2014.
31. Johan Eriksson, Giampiero Giacomello. **International Relations and Security in the Digital Age**. The united States of America: New York, published by Taylor and Francis E-Library, the first edition, 2007.
32. John Law: A Sociology of Monster, Essays On Power, Technology And Domination,(United Kingdom, London, published by Routledge, the first edition, 1991.
33. John Mearsheimer. "Structural Realism," ***in International Relation Theories, Discipline and Diversity***. Edited by Tim Dunne, Milja Kurki, Steve Smith. United Kingdom: published by Oxford University Press, the 3rd edition, 2013.

34. Joseph N. Pelton, Indu B. Singh**. Digital Defense, a Cybersecurity Primer** .Switzerland: published by Springer International Publishing, the first edition, 2015.
35. Joseph P. Farrell, Scott D. Hart. **Transhumanism, A Grimoire of Alchemical Agendas**, The United States of America: Washington, published by Feral House, the first edition, 2011.
36. Joseph Samuel Nye . ***Soft Power, The Means to Success in World Politics***. The Unites States of America: New York, published by PublicAffairs™, the first edition, 2004.
37. Joseph Samuel Nye. ***Power in the Global Information Age: From Realism to Globalization*** .United Kingdom: London, published by Routledge, the first edition, 2004.
38. Joseph Samuel Nye. ***Understanding International Conflicts: An Introduction to Theory and History*** . The united States of America: New York, published by Pearson and Addison Wesley, 4th edition, 2003.
39. Joseph Samuel Nye. ***Cyber Power***. The United States of America: Massachusetts, published by Belfer Center for Science and International Affairs, essay from The Future of Power in the 21st Century, 2010.
40. Juerg Studer. **Are There Five Rings or a Loop in Fourth Generation Warfare? A Study on the Application of Warden's or Boyd's Theories in 4GW**. The Unites States of America: Alabama, published by BiblioScholar, 2012.
41. Julie E, Mehan. **Cyberwar, Cyberterror, Cybercrime and Cyberactivism, an In-depth guide to the role of standards in the cybersecurity environment.** United Kingdom: Cambridgeshire business park, published by IT Governance Publishing, the 2nd edition, 2014.
42. Kevin D. Mitnick, William L. Simon **. The Art Of Deception, Controlling the Human Element of Security**. The United States of America: Ney york, published by John Wiley & Sons, the first edition, 2002.
43. Luo Zhiye. ***Sun Tzu's, The Art of War***. China: Beijing, published by The Foreign Translation Publishing House - The State Administration of Press, Publication, Radio, Film and Television of the People's Republic of China, 2007.
44. Martin Bauer. ***Resistance To New Technology, Nuclear Power, Information Technology and Biotechnology***, United Kingdom: Cambridge, Published by The Press Syndicate of The University of Cambridge, first paper edition with corrections, 1997.

45. Max G. Manwaring, ***The Strategic Logic of Contemporary Security Dilemma***. The United States of America: published by CreateSpace - U.S Army War College of Carlisle, 2012.
46. Max Weber. ***The Sociology of Charismatic Authority: Essays in Sociology trans***. The United States of America: New York, published by Oxford University Press, the first edition from the original essay in German (1921),1964.).
47. Michael Prosser, K.S Sitram. **Civic Discourse : Intercultural, International, and Global Media**. The United States of America: Stamford, published by Ablex Publishing Corporation, the first edition, volume 2, 1999.).
48. Michio Kaku. ***Parallel Worlds, A Journey Through Creation, Higher Dimension, and the Future of the Cosmos***. The United States of America: New York, published by DOUBLEDAY, 2004.
49. Michio kaku. ***Physics of the Impossible: A scientific Exploration into the World of Phasers, Force Field, Teleportation, and time travel***.The Unites States of America: Ney York, published by The Doubleday Broadway, the first edition, 2008.
50. Mordechai Guri, Assaf Lachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, Yval Elovici, GSMem . ***Data Exfiltration from Air-Gapped Computers over GSM Frequencies***. Negev, Published by Ben-Gurion University, edition 2015.
51. Nick Turse, The changing Face Of Empire: Special Ops, Drones, Spies, Proxy Fighter, Secret Bases, And Cyber Warfare. The Unites States of America: Chicago, published by Haymarket Books, the first edition 2012.
52. Norbert Wiener. ***Cybernetics, or Control and Communication in the Animal and the Machine***. The United States of America: Massachusetts, published by Massachusetts Institute of Technology, he 2nd edition, 1965.
53. Norbert Wiener. ***God and Golem Inc, a Comment on Certain Point Where Cybernetics Impinges on Religion***. The United States of America, Massachusetts, published by M.I.T Press, the first edition, 1964.
54. Norris Pippa. ***World Bank Staff Public Sentinel: News Media and Governance Reform***. The Unites States of America: Washington DC, Published by the World Bank, the first edition, 2010.
55. P.W Singer, Allan Friedman. **Cybersecurity and Cyberwar, What Everyone Needs to Know**. The United States of America: New York, published by Oxford University Press, the first edition 2011.

56. Paul Baran. ***On Distributed Communication, Introduction to Distributed Communication Networks***. The United States of America: Unites States Air Force, published by the Rand Corporation, 1964.
57. Penguin Classics, N. K. Sanders. **The Epic of Gilgamesh**. United Kingdom: London, Published by Penguin Books, Kindle Edition, 1973.
58. Prudence M. Rice. ***Maya Political Science، Time Astronomy and the Cosmos***. The United States of America: published by the University of Texas Press, the first edition, 2004.
59. R. U. Sirius, Jay Cornell. **Transcendence**: **The Disinformation Encyclopedia of Transhumanism And The Singularity**.The United States of America: San Francisco, published by Disinformation Books Red Wheel/Weiser LLC, the first edition 2015.
60. Richard A. Clarke, Robert K. Knake. **Cyber War the Next Threat to National Security and What to do about it**. The United States of America: Ney York, published by Ecco, the first edition, 2011.
61. Roger C. Molander, Andrew S. Riddile, Peter A. Wilson**. Strategic Information Warfare, A new Face of War**. The Unites States of America: published by RAND, 1996.
62. Ronald, R. Kline. ***The Cybernetics Moment, Or Why We Call Our Age The Information Age*** **.**The United States of America, Maryland, published by John Hopkins University Press, the first edition, 2015.
63. Saco Diana. "Colonizing Cyberspace: National Security and the Internet," in ***Cultures of Insecurity: States, Communities, and the Production of Danger*** . edited by Jutta Weldes, Mark Laffey, Hugh Gusterson, Raymond Duvall. The United States of America: Minnesota, published by the University of Minnesota Press, the first edition, 1999.
64. Samuel Glasstone, Philip J.Dolan. **The Effects of Nuclear Weapons** .The Unites States of America: published by The United States Department of Defense and The United States Department of Energy ,the third edition, 1977.
65. Serge S. Azarov, Alexander G. Dodonov. "Instrumental Corrections for a Definition of Cyberwar," in **NATO Security through Science Series - D: Information and Communication Security**. edited by Fernando Duarte Carvalho, Eduardo Mateus da Silva, Published by IOS Press Online, Volume 4, 2006, pp. 3-24.
66. Shane Harris. ***@War, The Rise of the Internet Military Complex***. The United States of America: New York, Published by the Library of Congress, The first edition, 2014.

67. Solange Ghernaouti. ***Cyber Power, Crime and Conflict and Security in Cyberspace***. Switzerland: Published by EPFL Press, the first edition, 2013.
68. Stephen J. Hines, Steven A. Seidman. "The Effect of Selected Cai Design Strategies on Achievement, and an Exploration of Other Related Factors," edited by Michael R. Simonson and Jacqueline Frederick. **10th Annual Proceedings of Selected Reserch Paper Presentation at the 1988 Annual Convention of the Association for Educational Communication and Technology**. The united States of America: Los Angeles, published by the educational Ressource Information Center, the first edition, 1988, pp. 372-383.
69. Tatiana Tropina, Cormac Callanan. **Self and Coregulation in Cybercrime, Cybersecurity and National Security** .The United States of America: New York, published by Springer Cham Heidelberg, in SpringerBriefs in Cybersecurity, the first edition, 2015.
70. Terry Terrif, Aaron Karp, Regina Karp. **Global Insurgency and the Future of Armored Conflict**, The Unites States of America: Ney York, published by Routledge, the first edition, 2008.
71. Torben Aegidius Mogensen . **Basics Of Compiler Design** . Denmark: Copenhagen, University of Copenhagen, published by the Department of Computer Science, the 10 years edition, 2010.
72. Walter, Warnick. David, Wojick. " A Missing Policy : Capacity Building for Sharing Scientific Knowledge," in **Science and Innovation Policy**, Atlanta Conference, Atlanta, GA, 2011.
73. William J. Mitchell . ***City of Bits: Space, Place, and the Infobahn***. The United States of America: Massachusetts, published by MIT Press, the first edition, 1996.

المذكرات:

0. Anthony F. Sinopoli. ***Cyberwar and International Law: An English School Perspective***, Master's Thesis. not published .University of South Florida: Scholar Commons Citation, 2012.
1. Brian Njama Kiboi. ***Cybersecurity as an Emerging Threat to Kenya's National Security***, Master's Thesis. not published. University of Pretoria: Department of Political Science, 2015.
2. Kjetil Tangen Gardåsen. ***Detecting Remote Administration Trojans through Dynamic Analysis using Finite-State Machines***, Master's Thesis. not published. Gjøvik University College: Department of Computer Science and Media Technology, 2014.

3. Michael Phillip Roush .***Securitization And Desecuritization In Estonia's Cyber Politics***, Master's Thesis. not published. University of South Florida: School of Social Sciences, 2015.
4. Nicholas C. Rueter. ***The Cybersecurity Dilemma***, Master's Thesis. not published. Duke University: Department of Political Science, 2011.
5. Rajbir Kaur Sidhu. ***Impacts of Geomagnetic storms on Trans-Canadian Grids***, Master's Thesis. not published. McGill University: Department of Electrical Engineering, 2010.

المقالات:

0. A.D Alberston, J. M. Thorson, S. A. Miske. "The Effect of Geomagnetic Storms on Electrical Power Systems," in IEEE Transactions on Power Apparatus and Systems, Volume PAS-93(1974), pp. 1031-1044.
1. Arnold Wolfers. "National Security as an Ambiguous Symbol," in Political Science Quarterly, No 4, Volume 67(December, 1952), pp, 481-502.
2. Attila Fernc Varga. "Rules of Engagements and International humanitarian Law," in LAW, No 1, Volume 11(2012), pp. 1-11.
3. Barry M.Leiner. Vinton G.Cerf, David D.Clark, Robert E.Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Posteln Larry G.Robertsn Stephen Wolff. "A Brief History of the Internet," in SIGCOMM Computer Communication Review, No 5, volume 39(October, 2009), pp. 22-31.
4. Beidleman Scott W. "Defining and Deterring Cyber War," in Military Technology, No 11, Volume 35(2011) 57-62.
5. Bin He Mitesh Patel, Zhen Zhang, Kevin Chen, Chuan Chang. "Accessing the Deep Web: A Survey," in Communications of the ACM, No 5, volume 50(May, 2007), pp. 95-101.
6. Brian TSAY. "The Tianhe-2 Supercomputer: Less than Meets the Eye?," in Newsletters(July, 2013), pp. 2-6.
7. Craig Smith, Ashraf Matrawy, Stanley Chow, Bassem Abdelaziz. "Computer Worms: Architectures, EvasionStrategies, and Detection Mechanisms," in Journal of Information Assurance and Security, No 4(2009), pp. 69-83.
8. D. Hollis. "Why States Need an International Law for Information Operations," in Lewis & Clark Law Review, volume 11(2007), p. 1023.
9. Daniel Stokols, Kara L Hall, Brandie K Taylor, Richard P Moser. "The Science of Team Science: Overview of the Field and Introduction to the Supplement," in American Journal of Preventive Medicine, No 2S, Volume 35(August, 2008), pp, 77-89.

10. Derek E. Bambauer. “Conundrum,” in Minnesota Law Review, No 227, Volume 96(2011), pp, 535-630.
11. Douglas Wikstrom. “A universally composable mix-net,” in Theory of Cryptography Conference (TCC), Volume 1(2004), pp. 317-335.
12. Edward Boxx. “Observations on the Air War in Syria,” in Air & Space Power Journal(March–April, 2013), pp. 147-168.
13. Eleanor Rieffel, Wolfgang Polak .“An Introduction to Quantum Computing for Non Physicists,” in Quant-Ph(Jeanery, 2000), pp. 1-45.
14. Erki Kodar. “Applying the Law of Armed Conflict to Cyber Attacks,” in ENDC Proceedings, Volume 15(2012), pp. 107-132.
15. Farwell James P, Rafal Rohozinski. “Stuxnet and the Future of Cyber War,” in Survival, No 1, Volume 53(2011), pp. 23-40.
16. Frank G. Hoffman. “Hybrid Warfare and Challenges,” in National Defense University Press, Volume – Issue 52(1st quarter, 2009), pp. 34-39.
17. Gary D. Brown. “Joint Force Quarterly,” in JFQ Marine Corps, issue 63, 4th quarter(October, 2011), p. 70-73.
18. Irving Lachow. “Cyber Terrorism: Menace or Myth?,” in A National Defense University and Forces Transformation and Resources Magazine(April, 2008), pp. 61-81.
19. Jack Dongarra. “Visit to the National University for Defense Technology Changsha, China,” in Oak Ridge National Laboratory(June 3, 2013), pp. 1-18.
20. Jeffrey Harton, Jennifer Seberry. “Computer Virusses an Introduction,” in Computer Science Communications, No 1, Volume 19(February, 1997), pp. 122-131.
21. Johan Eriksson, Giampiero Giacomello. “The Information Revolution, Security, and International Relation,” in International Political Science Review, No 3, Volume 27 (2006), pp. 212-224.
22. Joong Gyu Ha, Tom Page, Gisli Thorsteinsson. “A Study on Technophobia and Mobile Device Design,” in International Journal of Contents, No 2, Volume 7(Jun, 2011), pp. 17-25.
23. Joseph Carl Robnett Licklider, Welden E. Clar. “On-line Man-Computer Communication,” in AIEE-IRE, Spring Joint Computer Conference(May 1-3, 1962), pp. 113-128.
24. Keith Dowding. “Three-Dimensional Power: A Discussion of Steven Lukes’ Power: A Radical View,” in Political Studies Review, No 2, Volume 4(February, 2006), pp, 136-145.

25. Lene Hansen, Helen Nissenbaum. “Digital Disaster, Cyber Security, and the Copenhagen Schoo,” in International Studies Quarterly, Volume 53(2009), pp. 1175-1155.
26. Leonard Kleinrock. “An early History of the Internet,” in IEEE Communication, No 8, volume 48(August, 2010), pp. 26-36.
27. Lonsdale DJ. “Information Power: Strategy, Geopolitics, and the Fifth Dimension,” in Journal of Strategic Studies, No 2-3, Volume 22 (1999), pp.137-57.
28. Michael Burawory. “The Roots of Domination: Beyond Bourdieu and Gramsci,” in Sociology, No 2, Volume 42(2012), pp. 187-206.
29. Michael M. Bridges, Matthew P. Para, Michael J. Mashner. “Control System Architecture for Modular Prosthetic Limb,” in JOHNS HOPKINS APL TECHNICAL DIGEST, No 3, Volume 30(November, 2011), pp. 217-222.
30. Michael Scharf, Elizabeth Andersen, Effy Folberg, Michael Jacobson, Katlyn Kraus. “IS LAWFARE WORTH DEFINING?,” in Case Western Reserve Journal of International Law, No 11, Volume - Case 43(Sepetember, 2010), pp. 11-27.
31. Net Moran. “Understanding Advanced Persistent Threats,” in Login, No 4, Volume 36(August, 2011), pp. 21-26.
32. Nicholas Weaver, Vern Paxson, Stuart, Robert Cunningham. “A Taxonomy of Computer Worms,” in WORM, No 03(October, 2003), pp, 1-8.
33. Nick Bostrom. “A History of Transhumanist Thought,” in the Journal of Evolution & Technology, Volume 14(April, 2005), pp. 1-24.
34. Rid Thomas. “Cyber War Will Not Take Place,” in Journal of Strategic Studies, No 1, Volume 35 (2012), pp. 1-28.
35. ROBERT J. BUNKER. “Generations, Waves, and Epochs MODES OF WARFARE AND THE RPMA,” in AIRPOWER JOURNAL, No 1, Volume X (1996), pp. 1-10.
36. Robert M. Kitchin. “Towards Geographies of Cyberspace,” in Progress in Human Geography, No 3, volume 20(June, 1998), pp. 385-406.
37. Rudner M. “Cyber threats to critical national Infrastructure: An intelligence challenge,” in International Journal of Intelligence and Counterintelligence, Volume 26, (Marsh, 2013), pp. 453-481.
38. Sara Robinson. “Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders,” in SIAM News, No 5, Volume 36(June, 2003), pp. 1-4.
39. Scott Aaronson. “The Limits of Quantum,” in Information Technology Scientific American (Marche, 2008), pp. 62-69.

40. Sheldon JB. “Sate of the Art: Attacker and Targets in Cyberspace,” in the Journal of Military and Strategic Studies, Volume 12 (February, 2012), pp. 1-19.
41. Sweety Sen, Sonali Samanta, “INFORMATION SECURITY,” in The International Journal of Innovation research in Technology, No 11, Volume 1(2014), pp. 224-231.
42. Thomas X. Hammes. “Insurgency: Modern Warfare Evolves into a Fourth Generation,” in The Strategic Forum, No 214(January, 2005), pp. 1-8.
43. Tim Berners Lee, Robert Cailliaud, Ari Loutonen, Henrik Frystyk Nielsen, Arthur Secret. “The World Wide Web,” in Communication of the ACM, No 8, volume 37(August, 1994), pp. 76-82.
44. William S Lind, Keith Nightengale, John F Schmitt, Joseph W Sutton, Gary I Wilso. “The Changing Face of War: Into the Fourth Generation,” in Marine Corps Gazette (pre-1994), No 10, Volume 73(October, 1989), pp. 22-26.
45. William S. Lind. “Understanding Fourth Generation War,” in MILITARY REVIEW(September - October, 2004), pp, 12-16.
46. Yulia Cherdantseva, Jeremy Hilton. “Information Security and Information Assurance: Discussion about the Meaning, Scope, and Goals,” in Standars and Standarisation – Information Resources Management Association, Volume 3(2015), pp. 1204-1236.

المواقع الإلكترونية:

1. “Image of the Siemens S7-300,” in ***http://goo.gl/lB6zmp***.
2. “War in the fifth domain,” in: ***http://goo.gl/N6xi1U***.
3. 3D Model of the Liberator. in: ***http://defdist.tumblr.com/page/2*.**
4. A metal representation of the Bitcoin Currency, in: ***http://goo.gl/y4xnkQ*.**
5. Andy Greenberg. “3D Printed Gun’s Blueprints Downloaded 100,000 Time in Two Days,” in: ***http://goo.gl/RqGcOr*.**
6. Andy Greenberg. “Hacker Lexicon: What Is End-to-End Encryption?,” in: ***https://goo.gl/HRw386*.**
7. Anonymous Hacktivism.”DeepWeb Infography,” in: ***https://goo.gl/jAQqYR*.**
8. Becky Vanshur. “KC-135s refuel Idaho's A-10s in mid-flight,” in: ***http://goo.gl/plEVoD*.**
9. Bill Joy. “Why the future doesn’t Need Us,” in: ***http://goo.gl/1uFywu*.**
10. Brendan Koerner. “Why Do Surrendering Soldiers Wave White Flags?,” in: ***http://goo.gl/bFxFDa*.**
11. Chris Weigant. “We Need a Geneva Convention on Cyber Warfare,” in: ***http://goo.gl/cMcxKJ*.**

12. Clark Boyd. “Profile: Gary McKinnon,” in: ***http://goo.gl/5p6rN7*.**
13. David Axe. “How to Win a ‘Fifth-Generation’ War,” in: ***https://goo.gl/7lmMlq*.**
14. David Stupples. “The Next Big War Will Be Digital—and we’re not ready for It,” in: ***http://goo.gl/SqujuL*.**
15. Declan McCullagh. “Senate ratifies controversial cybercrime treaty,” in: ***http://goo.gl/m900FO*.**
16. Elisabeth Bumiller, Thom Shanker. “Panetta Warns of Dire Threat of Cyberattack.” in: ***http://goo.gl/WCm5Gv***.
17. Farnaz Fassihi. “Iran's Censors Tighten Grip,” in: ***http://goo.gl/3Htu80*.**
18. Franz-Stefan Gady. “A Geneva Convention for Cyberspace?,” in: ***http://goo.gl/PFRRrq*.**
19. Hold Security. “YOU HAVE BEEN HACKED!,” in: ***http://goo.gl/Y8Jq3m*.**
20. J.R. Wilson. “Cyber warfare ushers in 5th dimension of human conflict,” in: ***http://goo.gl/VpBVDu*.**
21. Jack Dongarra, Erich Strohmaier, Horst Simon. “the Top 500 List,” in: ***http://www.top500.org*.**
22. Jack Hitt. “The next battlefield may be in Outer Space,” in: ***http://goo.gl/lJ7kVG*.**
23. Jaganath Sankaran. “China’s Deceptively Weak Anti-Satellite Capabilities,”in: ***http://goo.gl/VP3Bas*.**
24. James Adams, “Virtual Defense.” in: ***https://goo.gl/tBbUvf***.
25. James Ball, Julian Borger, Glenn Greenwald. “Revealed: how US and UK spy agencies defeat internet privacy and security,” in: ***http://goo.gl/8FrMwd*.**
26. Jane Wakefield. “Can the government ban encryption,” in: ***http://goo.gl/irV6cu*.**
27. Jane Wakefield. “Can the government ban encryption,” in: ***http://goo.gl/irV6cu*.**
28. Jeff Larson. “The NSA’s Secret Campaign to Crack, Undermine Internet Security,” in: ***https://goo.gl/vm2VSJ*.**
29. Jonalan Brickey. “Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace,”in: ***https://goo.gl/Tu09Ml*.**
30. Karel Vereychken. “Les BRICS déclarent la guerre des câbles contre Londres et Wall Street,” in : ***http://goo.gl/HKGO13*.**
31. Larry Greenemeier. “Computers have a lot to learn from the human brain, engineers say,” in: ***http://goo.gl/dOW0sB*.**
32. Larry Jewell, Patrick Clancey, HyperWar Foundatio. “MANUALLY OPERATED MACHINE GUNS,” in: ***https://goo.gl/4xTB51*.**
33. Martin Slavík. “Mechatronics Studies in Europe,” in: ***http://goo.gl/u2hWfT*.**

34. Matthew Hutson. “How Much Can Your Brain Actually Process? Don’t Ask,” in: ***http://goo.gl/sornMi*.**
35. Michael Mimoso. “Google Completes Upgrade of its SSL Certificates to 2048-Bit RSA,” in: ***Https://goo.gl/zFCoc8*.**
36. Multi-barrel Weapons GAU-8/A 30MM Gatling Gun, in: ***http://goo.gl/d7cVNQ*.**
37. Nathan Thornburgh. “Inside the Chinese Hack Attack,” in: ***http://goo.gl/OoUalr*.**
38. Official Logo of Distributed Defense, in: ***https://defdist.org/*.**
39. Paul. “FBI’s Advice on Ransomware? Just Pay the Ransom,” in: ***https://goo.gl/3Qtjm8*.**
40. Piter Finn. “Cyber Assaults on Estonia Typify a New Battle Tactic,” in: ***http://goo.gl/w1zGHX*.**
41. Ranking Web of University, in: ***http://www.webometrics.info/en/Africa/Algeria*.**
42. Reto E. Haeni. “Information Warfare an introduction,” in: ***http://goo.gl/FCnKcN*.**
43. RHP. “The Heavy Gustav, Hitler and generals inspecting the largest caliber rifled weapon ever used in combat, 1941,” in: ***http://goo.gl/Wd0Cy6*.**
44. Samantha Dean. “The U.S Army Is Building an Iron Man Suit for Soldiers,” in: ***http://goo.gl/nkTToD*.**
45. Shouhuai Xu. “Cybersecurity Dynamics: A Foundation for the Science of Cyber Security,” in: ***http://www.cs.utsa.edu/~shxu/socs/*.**
46. Steve Ranger. “Organised cybercrime groups are now as powerful as nations,” **in: *http://goo.gl/3Kqi9X*.**
47. Steve Ranger. “Organized cybercrime groups are now as powerful as nations,” in: ***http://goo.gl/HiywTa*.**
48. Suzie Boss, “Integrated Studies: A Short History,” in: ***http://goo.gl/uNoeRm*.**
49. Valentin Mândrăşescu. “ BRICS countries are building a "new Internet" hidden from NSA,” in: ***http://goo.gl/HqYY0w*.**
50. Xiao Qiang. “How China’s Internet Police Control Speech on the Interne,” in: ***http://goo.gl/OlKtbx*.**

التقارير:

0. Greg Walton: China’s Golden Shield: Corporation and the Devlopement Surveillance Technology in the People’s Republic of China, (Canada, Montreal, published by The International Centre for Human Rights and Democratic Development, 2001.).

1. Kristin Finklea, Catharine A. Theohary: Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement, in CRS REPORT Prepared for members and Committees of Congress, January, 2015.
2. Steven R Gruchawka: Using the Deep Web: A How-To Guide for IT Professionals, (techdeepweb.com, published by Steven R Gruchawka, 2005.).
3. Vincenzo Ciancaglini, Marco Balduzzi, Robert McArdle, Martin Rösler: Below the Surface: Exploring the Deep Web (The Global Technical Support and R&D, Center of TREND MICRO, published by Trend Micro, 2015.).

المنشورات:

0. Akamai's, **[state of the internet] Q4 executive review**, 2015.
1. Broadband Commission for Digital Development, **Broadband for all a Report**, Switzerland, Geneva, 2015.
2. Council of Europe, **Convention on Cybercrime**, November, 2001.
3. FireEye, (https://www.FireEye.com), **Regional Advanced Threat Report**, Europe, Middle East and Africa 1H2014, 2014.
4. International Committee of the red Cross, **Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)**, Introduction to the Commentary on the Additional Protocols I and II, 8 June, 1977.
5. International Committee of the Red Cross, **Cyberwarfare and international humanitarian law: The ICRC's position**, June, 2013, pp. 1-4.
6. International Committee of the Red Cross, **What is International Humanitarian Law?** , Advisory Service on International Law, July, 2007.
7. National Aeronautics and Space Administration, Under the Foia case 51633, **Tempest: A Signal Problem, the story of the discovery of various compromising radiation from communication and Comsec equipment**, spectrum cryptologic field, 2007.
8. Suisse, Geneva, Academy of International Humanitarian Law and Human Rights**, Rules of Engagement**, October, 2011, p. 80.
9. United Nation, **Convention on Biological Diversity**, 1992.

النصوص القانونية:

0. United Stated Department of State, Bureau of Political-Military Affairs, office of Defense Trade controls compliance, Washington, D.C, ***A replay to Mr Cody Wilson about Distributed Defense***, 2013.
1. United States Constitution, ***Fifth Amendment of the United States Constitution***, 1789.
2. United States Constitution. ***Bill of right rectification, Second Amendment***, 1791.

الجرائد:

0. Stephan Hawking. "British Physicist Says Computer Viruses Should Be Considered as a Life Form." ***the Daily News***, No 116, volume 23, August, 1994.

الأشرطة المصورة:

0. Erin Lee Carr. "3D Printed Guns," Documentary in: ***https://youtu.be/DconsfGsXyA***, Motherboard, Vic Media Inc, (Sunday, May 29, 2016).
1. MMXII CO5 Interactive. "Stuxnet: Computer worm opens new era of warfare," Documentary in: ***https://youtu.be/6WmaZYJwJnq***, (Sunday, May 29, 2016).
2. Need to Know WLIW. "Stuxnet Virus," in: ***https://youtu.be/SAy46DhWW8Y***, (Sunday, 29 May 2016).

ينص جزء من القانون الأول لإسحاق نيوتن حول الحركة، على أن الجسم يضل في حركة مستمرة ودائمة، ما لم تؤثر قوة ما على هذا الجسم ؛ كذلك هي الهيمنة في ميدان العلاقات الدولية, فالهيمنة هي ذلك الجسم الذي لديه سلوك قياسي ثابت وهي بمثابة امتداد طبيعي للقوى على مختلف أشكالها، ومن جانب آخر, يمكن النظر إلى الأمن الإلكتروني, على أنه أحد تلك القوة التي تحاول إيقاف ذلك الجسم الذي تكلم عليه نيوتن، فمختلف هذه التفاعلات والتجاذبات، تترجم أرضا على شكل صراعات وتفاعلات بمختلف أشكالها، صراعات تعددت فيها الفواعل، الرسمية منها والغير رسمية، صراعات في ظل عالم متغير فرضته التقانة, والاكتشافات العلمية, وتغير الأفكار. فالتغيرات على الأرض كانت في عدة مناسبات بمثابة البيدق الذي ارتدت تأثيراته على مختلف المستويات، من تأثيرات على حقول التنظير، إلى تأثيرات في الواقع المعاش؛ فالأمن الإلكتروني جسد فعلا معادلة جديدة سيُجبر الجميع على التعامل معها، وفهمها، وذلك من أجل التمكن من فهم المعضلة الأمنية المعاصرة، كما من أجل ضبط ومعرفة مختلف الشرايين والأعصاب التي يقوم عليها الصراع من أجل الهيمنة العالمية حاليا، بالإضافة إلى محاولة تحسس نبض المستقبل القريب وفقا للمعطيات المتحصل عليها. وذلك في ظل نظرة جديدة، وطرق جديدة، ومقاربات أكثر تشابكا، وأكثر تداخلا، وأكثر عمقا في التعاطي مثل هذه المسائل، أو المعرفة بشكل عام.

| الأمن السيبراني | الدراسات المتداخلة | الحروب المتقدمة | الهيمنة الدولية | التقانة المتقدمة | الدراسات الأمنية | العلاقات الدولية |

Part of the first law of Isaac Newton about the motion state that an object either remains at rest or continues to move at a constant velocity, unless acted upon by a net force or affected by an external power. So are the constant search for acquiring the world domination in the field of international relations, and we can see it like a persistent and natural extension of various form of power. In the other hand Cyber security can be regarded as one of many powers or net forces that attempt to stop the continuum expansion of the above-mentioned objects as Newton's stated; those various reactions and interactions can be translated or understood by many forms of conflicts and events, in which both official and unofficial actors in IR can play a key role. Conflicts in a changing world imposed by technology and scientific discoveries and changing ideas, plus we easily perceive how a small change that occur in the ground, can be a pawn of an even bigger change in many domains, from the effects to international relations theory, to the close reality life effects. Indeed, Cyber security constitute a new element in the security equation to which everybody is forced to deal with in order to better understand the contemporary security paradox in addition to trying to feel the pulse of the near future by following new views and methodological approach, and by using a more deep, and complex analysis to those kinds of questions, or Knowledge in general.

| Cyber Security | Interdisciplinary studies | Advanced Warfare | Security Studies |

| International Hegemony |Advanced Technology | International Relations |