# الحروب الالكترونية: اللاتماثل في التهديد*

## *Cyber Wars: Asymmetric Threat*

*Baha Adnan ALSBARY***

***Abstract**:*
*The Asymmetric threat is considered one of the most challenges for stability in 21 centuries, that types of threat is conduct by player who has less capability and power comparing with states but at the same time it has ability to impose threats and create a new areas and instrument for combat. Cyber threat is one of asymmetric threat that should countered by states. It takes advantage particularly with increasing dependency on technology, internet and networks in directing military, security, and economic affairs.*

*The rapid technological and increasing dependency on technology and space in management of political economic and military affairs led to new conflicts, especially with current low level of cooperation and confrontation instruments, which is not enough to prevent new challenges or cyber threat. However, missing of coordination and cooperation among states in information security and cyber threat with absence of legal rules for monitoring and punish attackers make create obstacles in confrontation of cyber threat and difficulty to overthrowing it. So that cooperation and building legal rules to accounted of cyber-attack would be one of the most important factors in confronting the threat in addition increasing cultural, technological, and humanitarian awareness about the dangerous of cyber threats with increasing and improvements technical level of administration of materials and networks to protect it from cyber threats.*

***Keywords**: Cyber Threat, Information Security, Asymmetric Threat, Cyber Attack.*

**الملخص:**

تعد التهديدات اللامتماثلة أحد أهم تحديات الاستقرار في القرن الحادي و العشرين و التي أفرزت لاعبين و فواعل أقل قدرة و قوة من الدول، لكنها قادرة على فرض التهديد، فضلاً عن ابتكار مساحات و آليات جديدة لفرض التهديدات و منها التهديدات الالكترونية التي أصبحت أحد التحديات الرئيسة، التي فرضت على الدول ضرورة مواجهتها حتى إنها أصبحت أولويات عليا في استراتيجيات الدول الكبرى ، لاسيما في ظل تزايد الاعتماد على التكنولوجيا و الانترنيت و الشبكات في إدارة الشؤون العسكرية و الأمنية و الاقتصادية

* Makale Gönderiliş Tarihi: 14.05.2017. Yayına Kabul Tarihi: 02.05.2017
** Kofa Üniversitesi Öğretim Üyesi, alsabary2007@gmail.com.

فإن الحروب الالكترونية و إمكانية شن الهجمات أصبح امراً واقعياً و بالوقت نفسه يمثل تحدياً أمام الدول كونه يندرج تحت بند التهديدات اللامتماثلة و التي لا تحتاج الى قدرات او إمكانيات من أجل التنفيذ ، يتنوع التهديد الالكتروني بين التهديدات بسيطة المحتوى والنوع وحتى الدوافع والتي تكون احياناً فردية من حيث التنظيم وتستهدف في مواقع غير حساسة من حيث الاستهداف وأحيانا يكون الهدف منها إرضاء الذات واثبات القدرة، وهذا التهديدات لا تنجم عنها أضرار كبيرة في حين يصل مستوى التهديد من حيث التنظيم إلى إمكانية تحالف دول وتعاونها لشن هجوم الكتروني يستهدف مواقع حساسة ومهمة بالنسبة لسيادة الدول وأمنها القومي وغالباً ما يكون الدافع سياسي، أمنى او حتى اقتصادياً.

**الكلمات المفتاحية:** التهديدات الالكترونية، أمن المعلومات، التهديدات اللامتماثلة، الهجمات السيبرانية.

**المقدمة**

توقع كثير من المتخصصين أن توظيف التكنولوجيا في القطاعات السياسية و الأمنية و الاقتصادية سيسهم و يزيد من أطر التعاون و يرفع مستوى العلاقات الدولية ويقربها مختصراً الجهد و الوقت، وضمن الوظائف الاساسية للتكنولوجيا أنها حققت جزءاً من هذه الأهداف إلاّ أن الاستخدام الثنائي الجانب جعل من هذا القطاع عامل تهديد أو أنه يمكن أن يوظف بعكس ما كان مخطط له، أذ أسهم ظهور التكنولوجيا في إعادة تعريف العلاقات بين الدول، فقد اسهمت القفزات التكنولوجيا والتطور السريع في هذا المجال في ازدياد الحاجة و التوظيف له في كافة المجالات وكما هو متوقع فإن الترابط أصبح وثيقاً وإن الحاجة للتكنولوجيا للاستفادة منها أصبح أمراً لا يمكن الاستغناء عنه ، لكن الجوانب السلبية بهذا الثورة التكنولوجية أصبحت تشكل عائقاً وعامل ضغط، فظهور التهديدات و الحروب الالكترونية وتوظيف التكنولوجيا لإلحاق الضرر بالآخرين بطريقة غير شرعية، أعاد للأذهان ضرورة التفكير في كيفية تجنب الأضرار الناتجة من الاستخدام التكنولوجي في الشؤون السياسية والأمنية و حتى الاقتصادية، وقد أصبحت الهجمات الالكترونية واحدةً من أهم الأساليب التي تستخدم لأسباب عديدة كونها لا تحتاج الى كلف عالية او أنها غالباً ما تكون مجهولة المصدر وعدم القدرة على الكشف عن الجناة فضلاً عن أن الخسائر التي تسببها لا ترتبط بخسائر بشرية، وهذه عوامل مشجعة للاستخدام، كما أن التفوق في مثل هذه الهجمات لا يعتمد على مقاييس القوة وإنما يحتاج الى مهارة وتوظيف لهذه المهارة من قبل الأطراف الداعمة للهجوم . إن تقنية الوسائل الالكترونية التي تكون متاحة للكل ومنتشرة في الاسواق تجعل من السهولة اقتناءها، حتى وسائل الحماية والدفاع هي متوفرة بالتالي تستطيع الجهات المهاجمة توفيرها ومعرفة نقاط الضعف بها وذلك لن يكون

مكلفاً جداً مما يساعد على شن الهجمات.

**الإشكالية:** في ظل تزايد الاعتماد على التكنولوجيا و توظيفها في القطاعات السياسية و العسكرية و الاقتصادية أصبحت هذه القطاعات عرضةً للتهديد و الهجوم من خلال المنافذ الالكترونية و التهديد الالكتروني أصبحت اليوم وسيلة سياسية و أمنية و حتى اقتصادية يتم توظيفها لإلحاق الضرر بالآخرين ، لذلك فإن إشكالية البحث تمكن في أن الحروب الالكترونية اليوم هي شكل من أشكال الصراعات التي تستهدف الآخرين على التكنولوجيا كونها أقل تكلفة و لا تخضع لمعاير الصراعات التقليدية ، فضلاً عن أنها أصبحت وسيلة و سلاح بيد الدول يسهل استخدامه لإلحاق الضرر بالآخرين.

**الفرضية:** تنبثق فرضية الدراسة من معطيات الواقع الالكتروني وتسعى الدراسة لإثبات فرضية أساسية، وهي أن تزايد الاعتماد على التكنولوجيا في التعاملات والعلاقات على النطاق الدولي، في ظل ضعف التعاون والتنسيق السياسي والقانوني سيؤدي إلى تزايد الهجمات الالكترونية، التي تمتاز بأسلوب للهجوم مختلف من أساليب التهديد والهجوم التقليدية، فكلما زاد التطور والاعتماد التكنلوجي زادت احتمالية التهديد في هذا المجال.

**المنهجية:** سيتم الاستعانة بالمنهج التحليلي في بيان وتحليل ظاهرة التهديدات الالكترونية إلى مكوناتها السياسية لفهم الأساس والوسائل والنتائج فضلاً عن الاستعانة بالمنهج المقارن لدراسة بعض أوجه المقارنة مع الحالات التهديد والهجمات الالكترونية.

**المطلب الأول: اللاتماثل في الحرب الالكترونية**

تعد التهديدات اللامتماثلة أحد أهم تحديات الاستقرار في القرن الحادي و العشرين و التي أفرزت لاعبين و فواعل أقل قدرة و قوة من الدول، لكنها قادرة على فرض التهديد، فضلاً عن ابتكار مساحات و آليات جديدة لفرض التهديدات و منها التهديدات الالكترونية التي أصبحت أحد التحديات الرئيسية، التي فرضت على الدول ضرورة مواجهتا حتى إنها أصبحت أولويات عليا في استراتيجيات الدول الكبرى ، لاسيما في ظل تزايد الاعتماد على التكنولوجيا و الانترنيت و الشبكات في إدارة الشؤون العسكرية و الأمنية و الاقتصادية فإن الحروب الالكترونية و إمكانية شن الهجمات أصبح أمراً واقعياً، و بالوقت نفسه يمثل تحدياً أمام الدول كونه يندرج تحت بند التهديدات اللامتماثلة و التي لا تحتاج الى قدرت او إمكانيات من أجل التنفيذ.

فقد أصبحت الدول تدرك التطور السريع في التكنولوجيا و الاتصالات إذ نجدُ هناك طفرات في مجالات التكنولوجيا و المعلومات مما جعل من الصعوبة فهم كل هذه التحولات دفعة واحدة وهذا الأمر فرض تحدياً أمام الدول في كيفية الحفاظ على أمنها القومي أمام احتمالية تعرضها لهجمات الكترونية جديدة او مبتكرة لم تكن مستعدة للتعامل معها مسبقاً، إن التهديدات الالكترونية اليوم هي الأخطر في ظل التوسع و التطور لذي شهد هذا النوع و يمكن اعتبار الهجوم الالكتروني على المفاعل النووي الايراني عبر فيروس (Stuxnet) هو الأكثر تطوراً لان معظم الهجمات او الحروب الالكترونية تتم من خلال شبكة الانترنت وهذا الأمر يعدُّ مفتاحاً للاختراق، إلاّ أن هذا الهجوم استهدف أجهزة حاسوب غير مرتبطة بالأنترنت عبر زراعة برامج ممكن أن تكون حدثت من خلال شركة الصيانة المسؤولية عن الحاسبات الايرانية (سيماتك) وهي الشركة العالمية المتخصصة في مجال الأمن وإدارة المعلومات ولذلك فإن هذا الهجوم أبرز نوعاً مختلفاً من التهديدات الالكترونية.

فالإرهاب الالكتروني أحدث أنواع التهديدات التي يمكن أن تستهدف قطاعات عديدة، و يقول Gabriel Weimann (الباحث في معهد السلام الامريكي) إنَّ التهديدات الالكترونية زادت بعد أحداث ١١ ايلول ٢٠٠١ وأصبحت تمثل تحدياً حقيقياً أمام الولايات المتحدة و أنها انعكست سلبياً على انعدام الثقة بالتكنولوجيا و أساليب حمايتها فهذه التهديدات قادرة على استهداف البنى التحتية و الخدمات المالية و المصرفية، فضلاً عن أجهزة و مؤسسات الدول الأمنية ، ويذكر الكاتب أن الدولة قد تعمل على تحصين و تأمين فضائها الإلكتروني فيما يخص مؤسساتها العليا و الأمنية، إلاّ أن بعض المؤسسات الخاصة و الشركات متعددة الجنسية او البنى التحتية للدول تكون أكثر عرضةً للهجوم الالكتروني،[1] فالتهديدات الالكترونية قد تصل لقطاعات مؤثرة ومهمة ليس الأمنية منها فحسب، إنما حتى حركة الطيران وأجهزة مراقبه السدود والتحويلات المالية و المصرفية و طرق المواصلات و الخدمات التي تقدمها الحكومة للمواطنين، لأن معظم الدول الغربية و المتقدمة تقدم وتدير مؤسساتها عبر الشبكات و الأجهزة الالكترونية ، وهذا التوسع في القطاع الالكتروني ألهمَ و شجع الارهابين أفراداً كانوا ام مجموعات لشن هجماتهم من أجل تعطيل أو شل قطاعات معينة، لذلك فإن كل المخاوف و الإجراءات الاحترازية التي تسعى الحكومات الى تأمين نفسها الكترونياً هي مبررة ومعقولة نظراً لحجم التهديد على الرغم من كونه تهديداً غير منظور، فهذا النوع من التهديدات لا يكسب تعاطف المواطنين و تأييدهم أو حتى الحكومات كونها غير مرئية او غير مباشرة، فضلاً عن أن آثارها ونتائجها لا تمس الأفراد بصورة مباشرة وكغيرها من التهديدات اللامتماثلة فإن الارهاب الالكتروني يظهر عدم التناسب و التفاوت في القدرات واضحاً بين الذين يشنون الهجوم

1 Gabriel Weimann, *Cyber Terrorism How Real is The Threat?,* United States Institute of Peace, Special Report, NO:119, Washington, DC, USA, December 2004, p 2.

Baha Adnan ALSBARY

من حيث عددهم و إمكاناتهم وتكاليف التهديد وبين الجهات التي تتلقى التهديد من حيث الأثار التي يولدها زعزعة الاستقرار وتعريض أمنها للخطر، فضلاً عن أمن حلفائها او مؤسساتها وإن أصعب ما تمثله هذه التهديدات هو صعوبة تحديد الأطراف المسببة للهجوم، فمن الصعوبة معرفة مصدره هل هو فرد أم دولة ، فقبل أسابيع من الأزمة الجورجية و اقتحام القوات الروسية لها عام ٨٠٠٢ ، تعرضت جورجيا لهجمات الكترونية طالت مؤسسات رسمية و بنى تحتية كانت من الصعوبة معرفة الجهة التي تقف وراء الهجوم او الداعمة لها، على الرغم من تطابق الأسلوب مع هجمات التي شنت على استونيا عام ٧٠٠٢[٢] ، ويرى البروفسور(Nir B. Kshetri) الباحث في جامعة (North Carolina) بأنه حتى إذا كان من يقف وراء الهجمات السيبرانية هم أفراد فإن عدم التعاون بين الدول و الحكومات او إمكانية تحديد اماكنهم و ملاحقتهم يعد شيئاً صعباً، هذا إذا افترضنا بأنهم غير مدعومين او موظفين من قبل حكومات معينه، فمثلاً تتهم الولايات المتحدة روسيا و الصين بانهما لا يتعاونان معها، فضلاً عن عجزهما عن السيطرة على الهجمات الالكترونية التي تشن من أراضيهما، اذ كانت الهجمات التي شنت عام ٨٠٠٢ على موقع (Amazon) و مقره في الولايات المتحدة و المتخصص بتجارة التجزئة كانت من هكر روسي لم تستطع الولايات المتحدة القبض عليها، إلاّ عام ٢١٠٢ في قبرص و يُعزى ذلك الى عدم تعاون روسيا معها، حتى إن الحكومة الامريكية شككت بقدرة هذا الهكر بمفرده الى سعيه لمهاجمة مواقع عملاقة اضافة الى (e bay ، amazon، Priceline) فهو يحتاج الى امكانيات لا تستطع فرد واحد توفيرها.[٣]

على الرغم من أن الأهداف و النتائج واحدة بالنسبة للهجمات الإلكترونية فهي غالبا ما تكون مستهدفة من قبل الارهابين او ذوي المنافع الخاصة او الجماعات التي تبحث عن الحقوق العامة و محاربة الاحتكار فضلاً عن وحدة النتائج فهي بالنهاية تسبب التخريب و التهديد للدول، إلا أن الهجمات الالكترونية كأسلوب أصبح متنوع الأطراف و هو مختلف عن الهجمات الإرهابية التي تكون مدفوعة بأهداف سياسية، إلا أن الهجمات الإلكترونية أسبابها متنوعة مما يجعل الحكومات تعمل او تتوقع الهجوم من كل الأطراف، فأحيانا تكون دوافع الهجمات الإلكترونية سياسية و أمنيه و احياناً تكون دوافعها اقتصادية و احياناً اجتماعية و ثقافية و احياناً اخرى تكون من أجل التسلية و الهواية لكنها تسبب نفس النتائج و المخاطر على الدول أياً كان الدافع منها.

2 Anca Dinicu, *Cyber Threats to National Security. Specific Features and Actors Involved*, Nicolae Balcescu" Land Forces Academy, buletin scientific, NO:2, SIBIU, Romania, 2014, pp 110-111.

3 Nir Kshetri, Cybersecurity and International Relations: The U.S. Engagement with China and Russia, Prepared for FLACSO-ISA 2014, University of Buenos Aires, School of Economics, Buenos Aires, March, 10, 2017 http://web.isanet.org/Web/Conferences/FLACSO-, (Access Date: 09.10.2017).

إن التحدي الحقيقي يظهر أمام قدرات الدول و تطوير مهارتها في التصدي للهجمات الالكترونية مقابل التطور السريع و الهائل الذي يتمتع به المهاجمون، فالتهديد متنوع من مجرد قرصنة معلومات من قبل أفراد الى جريمة منظمة و هجمات الكترونية تمر بها دول، لذلك فإن مستوى الخطورة في ازياد فمع كل تطور تكنلوجي وتزايد الاعتماد على العالم الإلكتروني في إدارة المؤسسات و تقديم الخدمات يزداد معها احتمالية التعرض للهجوم ، ولأن التوسع في الخدمات الالكترونية أصبح أكثر شمولية فإن ذلك يكون دافعاً أمام المهاجمين لتنفيذ تهديداتهم، و تحدد التهديدات حسب طبيعتها وكما يبينها الشكل الآتي.

شكل 1 مصادر التهديد الالكتروني وأنواعه[٤]

| مصادر التهديد | الوصف |
|---|---|
| مشغلو شبكة البوت | مشغلو شبكة البوت هم قناصون، لكن بدلا من أن يتسللوا الى النظام مباشرة يتحكمون في العديد من الأنظمة لتنسيق الهجمات وتوزيع خطط التصيد والبريد العشوائي وهجمات البرمجيات الخبيثة. تتوفر خدمات هذه الشبكات احياناً في الاسواق السرية (مثل شراء هجوم منع الخدمة وخوادم ترحيل البريد وهجمات التصيد) |
| المجموعات الاجرامية | تسعى المجموعات الإجرامية الى مهاجمة النظم من أجل الحصول على المال وعلى وجه التحديد، تستخدم المجموعات الإجرامية المنظمة البريد العشوائي والتصيد وأنظمة التجسس البرمجيات الخبيثة لتنفيذ سرقة الهوية والاحتيال عبر الانترنيت. |
| عناصر ترعاهم الدولة | الحكومات الاجنبية والخدمات الاستخباراتية تستخدم الأدوات الالكترونية باعتبارها جزء من أنشطتهم الخاصة بجمع المعلومات والتجسس اضافة الى ذلك تعمل العديد من الدول وبشكل دؤوب على تطوير المبادئ والبرامج والامكانيات المستخدمة في حرب المعلومات. |

4 ستيوارت هايزو اخرون، الوجه المتقلب لأمن الفضاء الإلكتروني، مجلة ISACA، العدد:٦، ٢١٠٢، https:// www.isaca.org/Journal/archives/2012/Volume-6/Documents/12v6-The-Changing-Face-Arabic.pdf

| | |
|---|---|
| المخترقون (الهاكرز) | يخترق القراصنة الشبكات إما لإشباع رغبتهم في التحدي او من أجل نيل حقوق متبجحة في مجتمع المخترقين في حين إن الاختراق عن بعد كان يتطلب قدراً معقولاً من المهارات او المعرفة الحاسوبية، إلا أن الهواة ايضا يمكنهم الآن تنزيل نصوص وبروتوكولات الهجوم من على الانترنت وإطلاقها ضد المواقع التي تقع فريسة لهم |
| المطلعون على الاسرار الداخلية | يعتبر الموظف الساخط المطلع على الاسرار الداخلية لأي مؤسسة هو مصدر للجريمة الحاسوبية وقد لا يكون المطلعون على الأسرار الداخلية في حاجة الى قدر كبير من المعرفة بهجمات التسلل الحاسوبية لأن معرفتهم بالنظام المستهدف غالباً ما تتيح لهم إمكانية الوصول غير المقيد لإحداث ضرر بالنظام او سرقة بياناته، وتشمل هذه الفئة كذلك الموردين والموظفين الذين قد يدخلون البرمجيات الخبيثة بطريقة الخطأ الى أنظمتهم |
| المتصيدون | افراد او مجموعات صغيرة تقوم بتنفيذ خطط تصيد في محاولة لسرقة الهويات او معلومات تمهيداً للحصول على المال |
| مرسلو البريد العشوائي | افراد او منظمات تقوم بتوزيع رسائل غير مرغوب فيها تحمل معلومات خفية او مزورة لبيع منتجات او تنفيذ خطط التصيد او توزيع أنظمة تجسس / برمجيات خبيثة او الهجوم على المؤسسات (كهجمات منع الخدمة) |
| منشئو نظم التجسس / البرمجيات الخبيثة | افراد او منظمات تقوم بإنتاج وتوزيع أنظمة التجسس والبرمجيات الخبيثة احياناً مجاناً واحياناً اخرى تبيعها بأعلى سعر. |
| الارهابيون | يسعى الارهابيون الى تدمير البنى التحتية او اضعافها او استغلالها وذلك سعياً لتهديد الأمن الوطني او إيقاع إصابات جماعية او وضعية الاقتصادية العالمي والقضاء على الروح المعنوية والثقة |

وإدراكاً لتصاعد مستوى التهديد بدأت الدول تشير له علنا في استراتيجيتها الأمنية ففي تقرير حول تطبيق الاستراتيجية الأمنية الاوربية عام ٨٠٠٢ تضمن تهديدات غير تقليدية على غرار أمن الطاقة و التغيرات المناخية و الأمن السيبراني، إذ أصبح إدراك هذه التهديدات يُسهم في رسم سياسات الاتحاد الاوربي أمنياً و تحولت هذه الأخطار الى تهديدات أمنية بينما كانت تصنف سابقاً بأنها عمليات فردية ذات طابع مالي، الاّ

أنها أخذت مكانة اخرى في السياسات الاوربية بعد هجمات استونيا عام ٢٠٠٧ إذ لم يعد الهجوم الالكتروني له أهداف نفعية او مالية فقط بل سياسية و أمنية.[٥]

وتصنف التهديدات الالكترونية بصورة عامة الى أربعة أصناف:[٦]

١. اتلاف المعلومات او تغييرها: ويقصد به القدرة على الوصول الى المعلومات التي يمتلكها الخصم من خلال شبكة الانترنت والقيام بعمليات تغيير لتلك البيانات او إتلافها دون علم الخصم وهذا النوع يهدف الى تضليل الخصم.

٢. التجسس: تعني التجسس على شبكات الخصم دون أن يصاحب ذلك تدمير ويكون الهدف من ذلك الحصول على المعلومات المهمة.

٣. التجسس: تعني التجسس على شبكات الخصم دون أن يصاحب ذلك تدمير ويكون الهدف من ذلك الحصول على المعلومات المهمة.

٤. تدمير المعلومات: وهو أشد أنواع التهديد إذ يتم مسح وتدمير كافة المعلومات والبيانات الموجودة على الشبكة او الأجهزة.

لا تنشأ التهديدات الالكترونية من هجوم يشنه أفراد او منظمات او دول معينة فقط، أي ليس بسبب قوة الهجوم فحسب، إنما بسبب ضعف أنظمة الدفاع ايضاً، فإمكانية شن الهجمات هي نتيجة طبيعية لانخفاض مستوى الأمن الالكتروني، لكن تبقى إشكالية إنتاج برامج وأجهزة الكترونية غير قابلة للاختراق أمر غير متاح، فعلى الرغم من توافر الأفكار و المستلزمات و إنتاج إصدارات تعد مؤمنة إلا أن قدرة التهديد و تسارع اختراق هذه الإصدارات هو الآخر يمثل تطوراً في سياسات التهديد .وبهذا الاتجاه يذهب Joseph Nye فهو يرى أن من السهولة فرض الهيمنة البرية و البحرية للقوى الكبرى و أن انتشار الأساطيل والقوات رغم كلفتة و بطء التحرك مقارنة مع الفضاء الالكتروني، فإن فرض الهيمنة يعد أمراً مستحيلاً، فرغم إمكانية دول مثل الولايات المتحدة و الصين و روسيا إلاّ أنها ليس لديها القدرة على فرض السيطرة

5 تيري تاردي، الاتحاد الأوربي: مواجهة تهديدات غير تقليدية في عالم معلوم، في القوى العظمى والاستقرار الاستراتيجي في القرن الحادي والعشرين، رؤى متنافسة للنظام الدولي، تحرير جرائمي هيرد، دراسات مترجمة، العدد: ٠٦ مركز الامارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ٣١٠٢ ص ٩١٣.

6 محمد مختار، "هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية؟، مفاهيم لمستقبل"، ملحق شهري يصدر مع دورية اتجاهات الاحداث، العدد:٦، مركز المستقبل للأبحاث الدراسات المتقدمة، ابوظبي يناير ٥١٠٢، ص ص٥-٦.

على الفضاء الالكتروني.[٧]

إن استخدام التهديدات الالكترونية ليس بالضرورة أن تكون ذات أطر هجومية او تخريبه فبالإضافة الى الهجمات و التهديدات فهنالك نوع آخر من التهديد الذي يتم من خلال الشبكات، فالحملات و الدعم الالكتروني الذي يتم توفيره من حكومات معينة لشعوب دول اخرى لمناهضة أنظمتهم السياسية يعد نوعاً من انواع التهديدات الموجَّهة ضد الحكومات من قبل دول اخرى قبل ما حصل في ايران او مصر او بعض بلدان الثورات العربية التي حاولت حكومات هذه الدول قطع الشبكات او إضعافها، فبينما و فرت الدول الاخرى شبكات للتواصل او منصات الكترونية بديلة لدفع المواطنين للتعبير أكثر عن آرائهم عبر مواقع التواصل الاجتماعي، و يرى آخرين أن الاستهداف الالكتروني و التكنولوجي لم يعد يعني بالحكومات و الأنظمة السياسية فقط بل إن المواطنين أصبحوا أهدافاً لمثل هذه الهجمات عبر أجهزة التنصت و التجسس حتى إنها أصبحت أكثر قانونية في خلال التشريعات التي تخول الحكومات مراقبة البريد الالكتروني و التنصت على المحادثات و الاتصالات وحتى التعاملات الاقتصادية الالكترونية تحت مسوغ الأمن القومي، فقد استغلت الولايات المتحدة التهديدات المتكررة و استطاعت الحصول على تخويل من أجل المراقبة والتنصت.

ويرى Lawrence M. Friedman البروفيسور الذي كان يشغل منصب مدير إدارة المعهد الدولي للدراسات الاستراتيجية IISS ، أن التهديدات الالكترونية و إنْ كانت غير مرتبطة بأهداف معينة لكنها تسبب القلق و الارتباك للدول إذا ما نفذت و هو يرى أن الاهداف الكبرى و المواقع الحساسة التي من المفترض أن تكون أكثر حماية و تطور غير قابل للاختراق تكون هذه الاهداف مغرية أمام الهواة لإثبات قدرتهم و امكانياتهم للوصول الى أكثر المواقع سرية،[٨] لذلك احياناً يكون التهديد قادماً من أطراف ليس لها أي أهداف سوى الرغبة و إثبات الذات . ويرى Richard A. Clarke مستشار الأمن الالكتروني السابق في البيت الابيض أن التهديدات الالكترونية تعتمد على نقاط الضعف التي نستند عليها في تعاملاتنا الالكترونية فهو يرى أن برامج شركة Microsoft ضعيفة جداً وهي نقطة يستغلها الأعداء لشن الهجوم ويبرر ذلك في أن الشركة تتوخى بالدرجة الاساس من إصداراتها تحقيق الأرباح و ليس للحفاظ على أمن المعلومات، لذلك لابد من الانتباه لهذه النقطة فبرامج التكنولوجيا لا تكون مؤمنة بشكل جيد و إن على الولايات المتحدة أن لا تعتمد على هذه الشركات فقط في تحقيق أمنها الالكتروني لأنها أصبحت أكثر عرضة

7 Joseph Samuel Nye, *Cyber Power, Paper, Belfer Center for Science and International Affairs,* Harvard Kennedy School, Cambridge, Massachusetts, USA, May 2010, p 5-6.

8 لورنس فريدمان، "الثورة في الشؤون الاستراتيجية،" دراسات عالمية، العدد: ٠٣، مركز الامارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ٢٠٠٢، ص ٩٦.

للتهديدات لاعتمادها على برامج Windows[9]، بالمقابل فقد استخدمت الولايات المتحدة الفضاء الالكتروني من أجل تهديد بعض الدول و تعد ايران الهدف الاول بالنسبة للولايات المتحدة فقد تحول الفضاء الايراني الى ساحة قتال الكترونية و استخدمت الولايات المتحدة و اسرائيل أسلوب القوة الناعمة و الصلبة في إدارة هذه الحرب، إذ قامت بدعم الاحتجاجات الايرانية عام ٩٠٠٢ بعد الانتخابات الرئاسية من خلال فتح منصات الكترونية لدعم المعارضة و إيصال أصواتهم للخارج لمعرفة كيفية تعامل الحكومة معهم، وبالوقت نفسه استخدمت القوة الصلبة من خلال شن هجمات الالكترونية ضد البرنامج النووي الايراني من خلال فيروس (Stuxnet) الذي أصاب ما يقارب (٦١،٠٠٠الف) جهاز كمبيوتر تعمل ضمن البنى التحتية للبرنامج النووي الايراني لإلحاق الضرر بها،[10] في استطلاع للرأي أقامته إحدى الشركات الأمنية في الولايات المتحدة عام ٢٠٠٢ وجدت أن أكثر من ٧٠٪ من شركات الطاقة مستهدفه بهجمات الكترونية من أجل التحكم بها و بالخدمات التي تقدمها فشركات الكهرباء او الغاز او حتى المياه و السدود هي أهداف محتملة ومغريه بالنسبة للإرهاب الالكتروني[11] ولكن السؤال الأهم هنا لماذا هذه الأهداف ؟ ان التميز بين الأهداف من أجل مهاجمتها يعتمد بالدرجة الأساس على الجهة المهاجمة، فاستهداف هذه المواقع من أجل تخريبها لا يرتبط بالفوائد المالية او الاقتصادية، إنما مرتبط بمقاصد سياسية وأمنية بالدرجة الاساس او يرجع هذا التهديد او فرض التهديدات لأسباب عديدة:

١. ضعف التدابير القانونية على المستوى الدولي من أجل انشاء قواعد وطرق قانونية قادرة على محاسبة ومواجهة التهديدات الإلكترونية فصياغة التشريعات القانونية سيكون لها أثر كبير في الحد من التهديدات.

٢. قله التدابير والاجراءات التقنية والتي تتكون على مستوى يمنع اختراقها فالتهديدات الإلكترونية أكثر قدرة وتطور من اجهزة وبرامج الشبكات، او أنها تكون مصحوبة بنقاط ضعف مكشوفة تسهل اختراقها.

٣. قلة الوعي الإنساني فالكثير من التهديدات تتم من خلال الاحتيال على المستخدم للشبكات او الأجهزة، فالأمن السيبراني لا يتعلق فقط بأمن الحاسوب والشبكات، إنما لابد من بناء الوعي والثقافة بالتهديدات الالكترونية من أجل مواجهة وتطوير قدرات الفرد على أنواع وأساليب هذه التهديدات.

9 عباس بدران، الحرب الالكترونية الاشتباك في عالم المعلومات، بيروت، مركز دراسات الحكومة الالكترونية، ٢٠١٠، ص ١١.

10 عادل عبد الصادق، "القوة الالكترونية، اسلحة الانتشار الشامل في عصر الفضاء الالكتروني"، مجله السياسة الدولية، العدد:٨٨١، مؤسسة الاهرام للدراسات والبحوث الاستراتيجية، القاهرة ابريل ٢١٠٢، ص١٣.

11 James Andrew Lewis, *Assessing The Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies, Washington, D.C., USA, November, 2002, p 5.

Baha Adnan ALSBARY

٤. عدم وجود مؤسسات او منظمات قادرة على التعامل مع التهديدات الإلكترونية على مستوى الدولي فالهجمات والاحتيال وتدمير المعلومات والسرقة الالكترونية تحتاج الى شراكة دولية تنظم عملها من أجل مواجهة التهديد.

يذكر هنري كيسنجر في كتابه (النظام العالمي) إن الانترنت أصبح كل شيء وإننا على عتبة ((اشياء أنترنيتية)) او " انترنيت كل شيء" وهو يصف مدى التداخل والاعتماد على الانترنت والشبكات في إدارة أبسط الأمور اليومية ويذكر أن مستخدمو الهواتف النقالة الذكية يقدر عددهم بمليار وأنهم لديهم قدره تحليلية ومعلومات تفوق مستوى الاستخبارات قبل جيل واحد من الآن.[١٢]

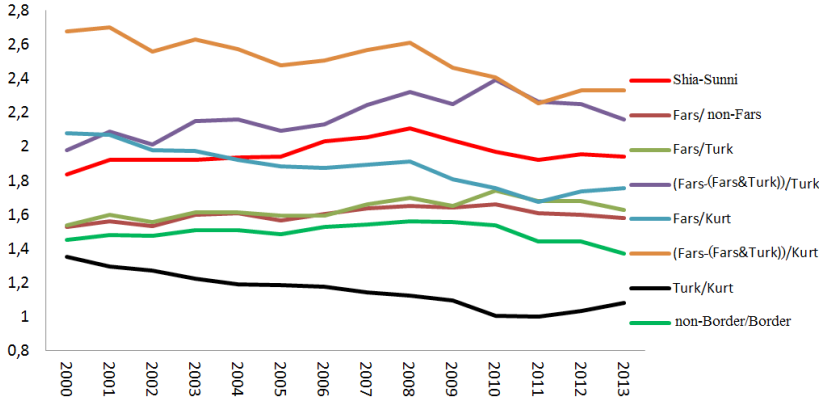
هذه الفكرة التي تكلم عنها كيسنجر توضح مدى التطور ومدى القفزات التي تحققت في الانترنت والتكنولوجيا في ظل اعتماد متزايد على عالم الشبكات والانترنت ويرى كسينجر أن تكنولوجيا الانترنت سبقت الاستراتيجية والعقيدة فلا يوجد تفسيرات منطقية ولا حتى أطر قابلة للتفسير، فلا يوجد مقاربات او أوجه متشابهة بين التكنولوجيا وقدرات الدول الأخرى، فجهاز حاسوب واحد قادر على إحداث فوضى عالمية.[١٣]

**المطلب الثاني: أساليب التهديد والمواجهة**

تدرك الأطراف المهاجمة ان التهديد الالكتروني من الصعوبة ردعه او مواجهته، فالسياسات العدوانية اللامتماثلة ومجهولة المصدر تبقى تشكل تحدياً أمام الدول، إذ تذكر هيلاري كلينتون وزير الخارجية الامريكي السابقه أن التهديدات الالكترونية أصبحت متطورة وأن القدرة على مواجهتها يحتاج على مواكبة التطورات وتذكر بأن المواقع الحساسة في الولايات المتحدة و التواصل الالكتروني كان عرضة يومياً لعمليات الاختراق من أجل سرقة المعلومات، و توكد أن الإجراءات بدائية او أنها من أجل الدفاع فقط، وهي تستشهد بالمواقف التي كانت تتعرض لها عند زيارتها الخارجية وطبيعة الإجراءات التقليدية لمواجهة التهديدات الالكترونية و تذكر أنها كانت تترك أجهزتها منزوعة البطاريات في الطائرة الخاصة و كذلك كانت تقرأ أي تعليمات تخص السياسيات المراد مناقشتها في الفندق في غرفتها وهي داخل خيمة غير شفافة من أجل منع التجسس عليها.[١٤]

12 هنري كيسنجر، النظام العالمي، تأملات حول طلائع الأمم ومسار التاريخ، ترجمة فاضل جتكر، دار الكتاب العربي، بيروت، ٥١٠٢، ص ٤٣٣.
13 المصدر السابق، ص ٦٣٣.
14 هيلاري كلينتون، خيارات صعبة، ترجمة ميري يونس، شركة المطبوعات للتوزيع والنشر، بيروت ٥١٠٢، ص ١٣٥-٣٣٥.

نمودار۷. نسبت درآمدهای سرانه نسبی گروههای مختلف هویتی به یکدیگر




هذه الخطوات تعني أنها إجراءات وقائية على الرغم من إدراك الدول الكبرى بالمشاكل و التهديدات للأمن الالكتروني حتى انها أصبحت تمثل أولوية في سياستها القومية، فمثلا نصت استراتيجية الأمن القومي البريطاني عام ٢٠١٠ على أن التهديدات الالكترونية أحد أكثر التهديدات الأمنية خطورة التي تواجها بريطانيا، إضافة الى الارهاب و الصراعات الإقليمية و الكوارث الطبيعية و قد خصصت ما يقارب ٦٥٠ مليون جنيه استرليني في ظل الأوضاع الاقتصادية التي تشهدها أوربا آنذاك للفترة ما بين ٢٠١١ الى ٢٠١٥ لتعزيز أمن الفضاء الالكتروني،[١٥] ويؤكد المتخصصون في أمن الفضاء أنه حتى في ظل الإجراءات الوقائية من أجل مواجهة التهديدات الالكترونية فإن احتمالية حدوث الخرق تبقى ممكنة وهو أسلوب تسعى اليه الجماعات التي تحاول إحداث الضرر، إذ تدرك الجماعات الارهابية أنها غير قادرة على المواجهة العسكرية و في ظل تزايد الحملات العسكرية ضدها و انحسارها جغرافيا، فإنها ستعمل على التحول نحو الهجمات غير التقليدية ولذلك فإنه من المحتمل زيادة هجماتها الالكترونية كأسلوب لإلحاق الضرر إذا تراجعت عسكرياً على أرض المعركة، فضلاً عن اعتمادها على الانترنيت و الشبكات العالمية من أجل التواصل مع مقاتليها او تجنيدهم او بث الفكر الارهابي وهم يستلهمون هذه الأفكار من مقدرة الأفراد على التسلل الى المنصات الالكترونية وقد تم على الوصول الى المعلومات و إدارة الأنشطة و الخدمات للدول وهم في بيوتهم، وقد ساهمت عولمة الشبكات الالكترونية و زيادة ترابطها في تشجيع الجماعات الارهابية على شن الهجوم من أجل الحاق أكبر قدر ممكن من الأضرار، لاسيما في ظل تطورات الخدمات الالكترونية التي أصبحت توفر إمكانية التخزين على الشبكات دون حفظ او خزن المعلومات على أقراص او أجهزة

15 جون باسيت حرب الفضاء الالكتروني، التسلح وأساليب الدفاع الجديدة، في الحروب المستقبلية في القرن الحادي والعشرين، مركز الامارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ٢٠١٤، ص. ٤٥-٥٥.

خارجية، وهذا ما زاد إمكانية الانتشار و التسلل للمعلومات، وإن قدرة الدول على حماية أمن المعلومات لكل الشعب و المؤسسات الخاصة أمر مستحيلاً فهي ليس لديها القدرة على متابعة كل شيء.

إن التهديد السيبراني لا يمثل خطراً الى الانترنيت فقط فنقاط الضعف تعد عاملاً مشجعا لارتكاب المزيد من الهجمات و التهديدات حتى إنها تكون دافعاً لتطوير الأنشطة الارهابية من الفائدة الفردية و المالية الى التوظيف الدول و التهديد الأمني و السياسي و الاقتصادي و على الرغم من العمل على مواجهة هذه التهديدات و التحديات غير التقليدية في العالم المتطور سريعاً، فإن ضعف الإجراءات وعدم التنسيق و التطور السريع في تقنيات الهجمات تجعل من الصعوبة التفوق، فمصادر التهديد أكثر قدرة و تطور في فرض سيطرتها، بالمقابل هم يكتشفون ويستغلون الضعف الحاصل في البرامج و الشبكات من أجل شن هجماتهم، وهذا الامر فرض تحدياً جديداً وكبيراً على الدول لاسيما المتقدمة منها في إضافة تهديد او بعد أمني للتهديدات غير المتماثلة.

لقد بدا الأمن السيبراني و تهديده يشكل تحدياً حقيقياً أمام الدول، فهي تدرك أن أمنها أصبح مرتبطاً بالتطور التكنولوجي وأن تعاملاتها الاقتصادية او الخدماتية مرتبطة ايضاً في هذا القطاع المعرض للتهديد بصورة مستمرة في البيئة الالكترونية الجديدة أصبح من الصعوبة الفصل بين العمليات الاستخبارية التي تقوم بها الحكومات لضمان و حماية أمنها القومي و بين العمليات التخريبية التي تقوم بها جماعات إرهابية لإلحاق الضرر بالآخرين،[16] ، فأحيانا يكون هدف التجسس من أجل مراقبة الأنشطة المشكوك بها او غير القانونية وهي جزء من إجراءات ضمان الأمن و احياناً تأخذ أشكال التهديد ، وهذا الأمر مرتبط بالدرجة الأساس بحسب طبيعة الاهداف المراد مراقبتها او اختراقها، فإن أيَّ اختراق للبرامج السرية التابعة للدول يعد عملاً إرهابياً، في حين إن أنشطة الشركات و الأشخاص عندما تراقب فأنها تكون عرضة للاحتمالين.

لقد أسهمت الثورة التكنولوجية و العولمة في مواجهة الأمن مما جعل من الصعوبة تحقيقه في ظل المعطيات التكنولوجية و الانفتاح مما جعل التهديدات تستغل نقاط الضعف للهجوم إذ ولدت تهديدات حديثة استغلت الدول التي كانت تبنى سياستها من أجل مواجهة التحديات المعروفة او التي يمكن إدراكها، لكن لأن عالم اليوم يتصف بالاستمرارية و التغيير و سرعة الابتكار مما جعل تهديدات مثل الارهاب و الجريمة من التهديدات التقليدية ، مقارنة مع التهديدات السيبرانية، فالدول المتقدمة بحكم حجم المصالح و عالمية التفاعلات الدولية فأنها تكون أكثر عرضة للتهديدات التي تتراوح الجهات المنفذة

16 عادل عبد الصادق، مصدر سبق ذكره، ص ٩٢.

لها ما بين الأفراد و القراصنة و الجماعات الإرهابية وصولاً الى الدول القومية، وهذا النطاق يمتد حسب طبيعة الأهداف المراد مهاجمتها، فضلاً عن أن هذه التهديدات تبقى احياناً من الصعوبة تحديد مكانها فأحيانا تأتي من دول حليفة او متعاونة مع بعضها، فمثلاً تعد رومانيا واحدة من الدول المتقدمة في مراكز الأمن السيبراني و مراقبة الهجمات، إلا أن بعض الهجمات تتم من خلال أجهزة حاسوب موجودة في رومانيا وتتم من قبل مهاجمين من دول اخرى يتسللون للحصول على IP من رومانيا لتنفيذ الهجوم،[١٧] مع ذلك هناك جهود دولية من أجل مواجهة هذه التهديدات و هنالك أفكار لوضع الأسس القانونية لمواجهة الجرائم الالكترونية، فقد تقدمت روسيا و الصين مسودة اقتراحات الى الامم المتحدة لوضع معيار قانوني سُمَّي (السلوك الدولي لأمن المعلومات) تتبنى منظمة شنغهاي تطبيقية لوضع قواعد و قوانين تحكم السلوك الدولي في الفضاء الالكتروني عام ١١٠٢، فيما قدمت روسيا عام ٥١٠٢ مشروع اتفاقية ( أمن المعلومات الدولية) و التي أكدت فيها الحاجة الى معاهدة فضاء الكتروني، فيما ناقش حلف شمال الاطلسي عام ٤١٠٢ تضمين المادة 5 من معاهدة الدفاع التي تنص على الدفاع الجماعي ضد التهديدات، لكي تنطبق على الهجمات الإلكترونية كذلك.[١٨]

لكن يبقى التعاون الدولي في هذا الإطار من أجل مواجهة التهديدات الإلكترونية ضعيفاً مقارنة مع حجم التهديد، فإجراءات المواجهة و التعاون لا ترتقي لجم التهديد، فمثلاً تتهم الصين الولايات المتحدة بعدم الجدية و التعاون معها فيما يتعلق بجرائم التهديدات الإلكترونية و إن طلبات التعاون التي ترسلها الصين الى الولايات المتحدة بخصوص التهديدات الإلكترونية عبر مكتب التحقيقات الفيدرالية FBI لا تتلقى منها الرد، وإن عدم التعاون يعكس رغبة الولايات المتحدة في توظيف قوتها التكنولوجية ضد الصين، حتى إنها كانت أهدفاً لهجمات شنت من الأراضي الأمريكية، الأكثر من ذلك أن الصين ترى أنَّ وكاله الاستخبارات المركزية CIA توظف شركات تكنولوجية لشن هجمات الكترونية لصالحها، وتتهم الصين شركة مايكروسوفت MICROSOFT بأنها تتعاون مع الاستخبارات الامريكية لزرع برامج خبيثة و أجهزة تنصت للمنتوجات التي ترسل للصين.[١٩]

إن ظهور صراعات الكترونية و حرب من هذا النوع قد يدفع بعض الأطراف الى بناء تحالفات الكترونية، أما من أجل الهجوم او الدفاع فمثلا ترى الولايات المتحدة أن الصين و روسيا يسعيان لبناء تحالف الكتروني

17 Lewis, Ibid, p. 4.

18 Vladimir Radunović, Cyberspace and International Peace and Security, Webinar Series Training Summary, JUNE 2015, http://www.gp-digital.org/wp-content/uploads/pubs/gccs2015%20collated%20webinar%20summaries%20final.pdf, (Access Date: 20,09.2017).

19 Kshetri, Ibid, p. 12.

من أجل شن المزيد من الهجمات، وأن هذا التحالف يسعى لكسب حلفاء جدد و توظيفهم، فمثلاً ان الهجوم على شركة ((SONY الامريكية تتهم به الولايات المتحدة كوريا الشمالية بتنفيذه ولكن مثل هذا النوع من الهجمات لا تملك كوريا الشمالية الإمكانيات لتنفيذه بمفردها، بالتالي قد تكون الصين هي من ساعدت كوريا الشمالية بالتكنولوجيا من أجل شن الهجوم،[٢٠] أي أن احتمالية ظهور تحالفات الكترونية أمر ممكن و كذلك قد تشهد تحالفات هجومية او دفاعية مثلما قررت الدول الاوربية إنشاء وحدات الدفاع الالكترونية ضمن حلف الناتو لتنسيق الدفاع الالكتروني ضد احتمالية تعرضها لهجمات إرهابية.[٢١]

فيما تعد اسرائيل أحد أكبر الدول تعرضاً و تنفيذاً للهجمات الالكترونية، فهي تعرضت لهجمات مختلفة المصادر كان أشدها يوم ٧ نيسان عام ٣١٠٢ حين تعرضت مواقع و صفحات مؤسسات اسرائيلية ذات طبيعة سياسيه و أمنيه و إعلامية الى أكبر هجوم الكتروني نفذته مجموعة الانونميس و التي توصف بأنها من أكبر المجموعات الالكترونية تأثيراً في العالم و لديها القدرة على شن هجمات الكترونية،[٢٢] هذه الهجمات التي طالت مواقع إسرائيلية دفعتها للرد بأسلوب مغاير، فهي من الدول التي أسست وكالة استخبارات متخصصة وهي "الهيئة القومية للحرب الالكتروني" لمواجهة التهديدات وقد ردت اسرائيل على الهجمات عبر أسلوب تركيز القوة (BANDWIDTH) الذي يعني توظيف كل الأجهزة الالكترونية المدنية في خدمة الدولة من أجل إدارتها مركزياً لشن الهجوم الالكتروني عبر مساهمة الأمن الأجهزة و مجموعة كبيرة من منافذ الانترنت لشن الهجوم و تريد اسرائيل من ذلك تركيز الهجمات بيد المؤسسات و عدم الاعتماد على العمل الفردي او الشعبي وهي بذلك مثل الذي يسلط قوة إشعاع مكثفة (ليزر) أمام الضوء العادي،[٢٣] في عام ٨٠٠٢ يقول نائب وزير الدفاع الأمريكي آنذاك William J. Lynn بينما كانت وزارة الاستخبارات المركزية تعتقد أنها تستخدم أفضل نظم الحماية فيما يتعلق بسرية المعلومات العسكرية لاسيما أنظمة التطوير و الابتكار للمقاتلات الحربية الامريكية F-35 و التي وصلت تكلفة تطوير النموذج الى ٠٠٣ مليار دولار، فإنه تم اكتشاف نظم تشغيلية يتم التحكم بها عن بعد موجوداً في حواسيب الأجهزة التشغيلية لبرامج التطوير.[٢٤]

20 دعاء الجهيني طريق محتمل لمواجهة تهديدات الفضاء الالكتروني؟، مفاهيم المستقبل"، ملحق شهري يصدر مع دورية اتجاهات الاحداث، العدد:٦، مركز المستقبل للأبحاث الدراسات المتقدمة، أبو ظبي، يناير ٥١٠٢، ص ٢١.

21 المصدر السابق، ص ٢١.

22 خالد وليد محمود، الهجمات عبر الانترنت، ساحة الصراع الالكتروني الجديد، سلسلة دراسات، المركز العربي للأبحاث ودراسة السياسات، أبو ظبي، سبتمبر ٣١٠٢، ص ١٢.

23 عباس بدران، مصدر سبق ذكره، ص ٤٤.

24 Shmuel Even and David Siman-Tov, Cyber Warfare: Concepts and Strategic Trends, Memorandum No:117, *Institute for National Security Studies,* May 2012, https://www.files.ethz.ch/isn/152953/inss%20memorandum_may2012_nr117.pdf, (Access Date: 01.10.2017).

لذلك على الحكومات إذ ارادت ان تحافظ على أمنها القومي من التهديدات الالكترونية، يجب أن تتغير التقنيات التي تؤثر على الأمن السيبراني للدول بشكل كبير بأن تتحول من الحلول البسيطة مثل مضادات الفيروسات إلى تقنيات أكثر تطوراً من الحلول للعمل على مواجهة هذه التهديدات التي تزداد تعقيداً.

**الخاتمة والاستنتاج**

على الرغم من التاريخ القصير للتهديدات الالكترونية إلا أنه لابد من بناء وعي كبير و متزايد من خطورة هذه التهديدات، فالتهديدات الالكترونية أصبحت متطورة من حيث أشكالها بين سرقة الأموال و الاحتيال و التجسس و سرقة الابتكار وصولاً الى التهديدات البنى التحتية و سرقة معلومات الدولة الأمنية و العسكرية وحتى الاقتصادية واختلف كذلك من حيث التجسس و السرقة الى الهجوم و التدمير و التحكم بها إضافة الى بعد آخر وهو ابتكار قنوات للهجوم حديثة من شبكات الانترنت الى توظيف الأجهزة و زرع برامج بداخلها للتجسس وصولاً الى اختراع وسائل للتهديد بعيدة عن ذلك مثلما حدث مع فيروس (Stuxnet) وهذا الأمر يعد بمستقبل من التهديدات غير المسبوقة التي يمكن أن تشكل تحدياً آخر أمام الدول لحمايتها الإلكترونية كونه فضاء يتميز بالسهولة وقلة التكلفة لخوض حروب و تهديدات جديدة.

إن زيادة التفاعلات الالكترونية في ظل التطور التكنولوجي تجعل من الصعوبة التحكم به و السيطرة عليه من قبل أيَّة جهة، ففي ظل تنوع الجهات الصانعة و المستخدمة للتكنولوجية وفي ظل تنوع الاستخدامات التكنولوجية يصبح من المستحيل مراقبة كل الآليات التي تمر بها هذه العلمية وبذلك تكون هذه الشبكات و الأجهزة و المنافذ الالكترونية عرضة للتوظيف من أجل شن هجمات الكترونية الهدف منها إلحاق الضرر بالخصم، فبغض النظر عن الغاية من الهجوم و بغض النظر عن الأهداف المراد مهاجمتها و طبيعة الأضرار الناجمة من الهجوم، فإن التوظيف الثنائي للتكنولوجيا و إخراجها من إطار تعزيز التعاون الى أطر الصراع و التهديد يعد مجالاً جديداً في سياسات الدول، مما يفرض نمط جديد من التفاعلات.

يتنوع التهديد الالكتروني بين التهديدات بسيطة المحتوى والنوع وحتى الدوافع والتي تكون احياناً فردية من حيث التنظيم وتستهدف في مواقع غير حساسة من حيث الاستهداف وأحيانا يكون الهدف منها إرضاء الذات واثبات القدرة، وهذا التهديدات لا تنجم عنها أضرار كبيرة في حين يصل مستوى التهديد من حيث التنظيم إلى إمكانية تحالف دول وتعاونها لشن هجوم الكتروني يستهدف مواقع حساسة ومهمة بالنسبة لسيادة الدول وأمنها القومي وغالباً ما يكون الدافع سياسياً او أمنياً او حتى اقتصادياً.

لقد شكل ظهور هذا النوع غير المتماثل من التهديد أُطراً جديدة لإدارة التفاعلات والسياسات بين الدول فهذا الحقل والمجال الواسع من التهديد والذي لا يحتاج الى كلف مرتفعة، فضلا الى صعوبة معرفة مصدر التهديد ولا حتى إمكانية تعقبه، ويبقى هذا النوع من التهديدات المفضلة لدى الدول.

إن التسارع التكنولوجي وتوسع مجالات الإنتاج وتزايد الاعتمادية على التكنولوجيا والفضاء لإدارة الشؤون السياسية و الاقتصادية و حتى العسكرية تنذر بنوع جديد من الصراعات، لاسيما أن التعاون و آليات المواجهة ليست قوية بالقدر الذي يمنع ظهور تحديات او تهديدات الكترونية جديدة، و إنَّ عدم التنسيق و التعاون بين الدول في مجال أمن المعلومات و التهديدات السيبرانية وفي ظل غياب قواعد قانونية لمراقبة و معاقبة المهاجمين تجعل من إمكانية القضاء على هذه التهديدات او حتى مواجهتها أمراً مُستبعداً في ظل هذه المعطيات، أي أن التعاون و بناء و تشريع قواعد قانونية لتجريم و محاسبة الهجمات الالكترونية سيكون أحد أهم الوسائل لمواجهة التهديد، فضلاً عن زيادة الوعي الثقافي و التكنلوجي الإنساني بمخاطر التهديدات الالكترونية و العمل على زيادة و تحسين المستوى الفني و التقني لإدارة الأجهزة و الشبكات الالكترونية لحمايتها من مخاطر التهديدات الالكترونية.

**قائمة المصادر**

**أولاً: العربية**

تيري تاردي، الاتحاد الأوربي: مواجهة تهديدات غير تقليدية في عالم معلوم، في القوى العظمى والاستقرار الاستراتيجي في القرن الحادي والعشرين، رؤى متنافسة للنظام الدولي، تحرير جرايمي هيرد، دراسات مترجمة، العدد:٠٦، مركز الامارات للدراسات والبحوث الاستراتيجية، أبو ظبي ٣١٠٢.

جون باسيت، حرب الفضاء الالكتروني، التسلح وأساليب الدفاع الجديدة، في الحروب المستقبلية في القرن الحادي والعشرين، مركز الامارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ٤١٠٢.

خالد وليد محمود، الهجمات عبر الانترنت، ساحة الصراع الالكتروني الجديد، سلسلة دراسات، المركز العربي للأبحاث ودراسة السياسات، أبوظبي، سبتمبر ٣١٠٢.

دعاء الجهيني، طريق محتمل لمواجهة تهديدات الفضاء الالكتروني؟، مفاهيم المستقبل، ملحق شهري يصدر مع دورية اتجاهات الاحداث، العدد:٦، مركز المستقبل للأبحاث الدراسات المتقدمة، أبوظبي، يناير ٥١٠٢.

عادل عبد الصادق، "القوة الالكترونية، اسلحة الانتشار الشامل في عصر الفضاء الالكتروني"، مجله السياسة الدولية، العدد:٨٨١، مؤسسة الاهرام للدراسات والبحوث الاستراتيجية، القاهرة، ابريل ٢١٠٢.

عباس بدران، الحرب الالكترونية الاشتباك في عالم المعلومات، مركز دراسات الحكومة الالكترونية، بيروت، ٠١٠٢.

لورنس فريدمان، الثورة في الشؤون الاستراتيجية، دراسات عالمية، العدد:٠٣، أبو ظبي، مركز الامارات للدراسات والبحوث الاستراتيجية، ٠٠٠٢.

محمد مختار، هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية؟، مفاهيم لمستقبل، ملحق شهري يصدر مع دورية اتجاهات الاحداث، العدد:٦، مركز المستقبل للأبحاث الدراسات المتقدمة، ابوظبي، يناير ٥١٠٢.

هنري كيسنجر، النظام العالمي، تأملات حول طلائع الأمم ومسار التاريخ، ترجمة فاضل جتكر، دار الكتاب العربي، بيروت، ٥١٠٢.

هيلاري كلينتون، خيارات صعبة، ترجمة ميري يونس، شركة المطبوعات للتوزيع والنشر بيروت، ٥١٠٢.

**ثانياً: الأجنبية**

DINICU, Anca, *Cyber Threats to National Security. Specific Features and Actors Involved,* Nicolae Balcescu" Land Forces, buletin scientific, NO:2, Academy, SIBIU, Romania, 2014.

EVEN, Shmuel and SIMAN-TOV David, Cyber Warfare: Concepts and Strategic Trends, Memorandum No:117, Institute for National Security Studies, May 2012, https://www.files.ethz.ch/isn/152953/inss%20memorandum_may2012_nr117.pdf, (Access Date: 01.10.2017).

Gabriel Weimann, *Cyber Terrorism How Real is The Threat?,* United States Institute of Peace, Special Report, NO:119, Washington, DC, USA, December 2004.

Joseph Samuel Nye, *Cyber Power, Paper, Belfer Center for Science and International Affairs,* Harvard Kennedy School, Cambridge, Massachusetts, USA, May 2010.

LEWIS James Andrew., Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats: report, Center for Strategic and International Studies, Washington, D.C., USA, November, 2002.

Nir Kshetri, Cybersecurity and International Relations: The U.S. Engagement with China and Russia, Prepared for FLACSO-ISA 2014, University of Buenos Aires, School of Economics, Buenos Aires, March, 10, 2017 http://web.isanet.org/Web/Conferences/FLACSO-ISA%20BuenosAires%202014/Archive/6f9b6b91-0f33-4956-89fc-f9a9cde89caf.pdf, (Access Date: 08.09.2017).

RADUNOVIĆ Vladimir, Cyberspace and International Peace and Security, Webinar Series Training Summary, JUNE 2015, http://www.gp-digital.org/wp-content/uploads/pubs/gccs2015%20collated%20webinar%20summaries%20final.pdf, (Access Date: 20,09.2017).

## Structured Summary

The rapid development of cyber technology considered main challenge that faces states in its effort to counter it. The new skills and technologies of cyber-attacks combined with spread of dependency on technology in all life aspect make state institutions more susceptible to cyber-attacks.

The motivation of cyber-attacks differs from motivation of terrorism because terrorists focus on political purposes. However, the cyber-attacks have variety in terms of aggressors whose may be individuals, groups, states as well as variety in purposes, which could be political, economic, cultural and social aims so the governments should expect attack from different parties, however regardless its motivations or goals the cyber attack is threat that should be counter and overcome by state.

The internet is not the only area of cyber threat. The weakness points in networks and programs considered an assistant factor for more attack of different types of cyber threat it also could be a motivation for terrorist activity and political, economic and security threat. The miss of coordination and rapid development in cyber technology create a challenged environment even for developed states in its conformation to cyber attack, these form Asymmetric threats create a new framework for political interaction among state. The main characterizes of cyber threat as low cost and difficulty to discovered or tracked make it the best chose for aggressor states. So that if the governments want to protect its national security from it than they should develop the technology of cyber security which mean it should transform from using traditional technology as antivirus to more develop technology to defeat that complexity of cyber threats.

Many scholars believe that deploying of technology in political, security and economic sectors would contribute in increasing cooperation frameworks of International Relation. However, technology has achieved some of that goal, it redefines the International Relations, and it becomes one of the main feature of International Relations through as it used as a necessary tool in all aspects of International Relation. However, using of technology is not good absolutely because it has some negative aspects of as cyber threat and cyber wars, which led to rethinking about depending on technology in political, security and economic sectors of International Relations. The Asymmetric threat is considered one of the most challenges for stability in 21 centuries,

that types of threat is conducted by player who has less capability and power comparing with states but at the same time it has ability to impose threats and create a new areas and instrument for combat. Cyber threat is one of asymmetric threat that should be countered by states. It takes advantage particularly with increasing dependency on technology, internet and networks in directing military, security, and economic affairs.

In spite of the short history of electronic threats, there is a need to build a large and growing awareness of the seriousness of these threats. Electronic threats have become sophisticated in terms of their forms between money theft, fraud, espionage, theft of innovation, threats to infrastructure, theft of state security and military information even the economic differed in terms of espionage and theft to the attack and destruction and their control as well as after, another innovation channels modern attack from online networks to employ devices and transplant programs inside them to spy down to the invention of the means to threaten far from it, as happened with P Leros (Stuxnet) and this is the future of the unprecedented threats that could pose another challenge for States to protect the electronic space is characterized by being easy and low cost to fight wars and new threats.

The increase of electronic interactions in the light of technological development makes it difficult to control and control by any party, because the diversity of manufacturers and uses of technology and in the diversity of technological uses it becomes impossible to monitor all the mechanisms that pass through this scientific and so these networks and electronic devices and ports vulnerable to employ in order to launch electronic attacks intended to inflict damage to the opponent, apart from the purpose of the attack and regardless of the targets to be attacked and the nature of the damage caused by the attack, the bilateral recruitment technology and take it out of the framework of strengthening Cooperation frameworks to the conflict and the threat is a new area in the policies of States, which imposes a new pattern of interactions.

The electronic threat varies from simple threats to content, type, and even motivations, which are sometimes individualized in terms of organization and targeted at sites that are not sensitive in terms of targeting and are sometimes intended to satisfy themselves and prove capability. These threats do not cause significant damage, the possibility of coalition countries and their cooperation to launch an electronic attack targeting a sensitive and important site for state sovereignty and national security, and often politically motivated or security or even economically.

The emergence of this asymmetric type of threat has created new frameworks for managing interstate interactions and policies. This field, the wide range of threat, which does not require high costs, the difficulty of knowing the source of the threat and not even the possibility of tracking it.

Technological acceleration, expansion of production areas, and increasing dependence on technology and space for the management of political, economic, and even military affairs foreshadow a new type of conflict, especially as cooperation and coping mechanisms are not as strong as the emergence of new electronic challenges orthreats. States in the field of information security and cyber threats In the absence of legal rules to monitor and punish the attackers make it possible to eliminate these threats or even to face them is unlikely in light of these data, that is, the cooperation and the construction and legislation of legal rules to conduct Accounting and cyber-attacks will be one of the most important means to counter the threat, as well as increasing cultural awareness and humanitarian risks of technological electronic threats and to increase and improve the technical level and technical management devices and electronic networks to protect them from the dangers of electronic threats.