دور الإستراتيجيات الإستباقية في مواجهة الهجمات السيبرانية - الرّدع السيبراني أنموذجا -

The role of proactive strategies in the face of cyber attacks - cyber-deterrence model -

ط. د. سامي محمد بونيف، طالب باحث في الدكتوراه،
جامعة الجزائر 03، الجزائر.

ملخص:

إثر أحداث 11 سبتمبر 2001 م وجدت الولايات المتحدة الأمريكية نفسها أمام أخطار جديدة أعلى مستوى مما كان إبان الحرب الباردة ، فالأمر أصبح لا يتعلق بمواجهة طرف مماثل بل جماعات غير خاضعة لأي سلطة و حتى تهديدات أخرى لم تعهد من قبل ، مما جعلها تتجه لأساليب جديدة لمجابهة الخطر القائم و ما قبله و محاولة الاستباق و لو بخطوه مما يزيد من نجاعة الأساليب الدفاعية ، و هنا تبرز أهمية الطرق الوقائية خاصة إذا ما تعلق الأمر بتهديدات متغيرة و متطورة مثل المجالات السيبرانية التي أصبحت أحد أهم مظاهر الحياة الإنسانية و أحد الأدوات الأساسية في إستراتيجيات الدول .

مما لا شك فيه أن أمن المعلومات يعد أحد الخطوط الحمراء التي تمس بالأمن القومي بما لها ارتباط شبكي بالقطاعات الحيوية لدى الدولة ، مما تطلب وجود إستراتيجيات استباقية للوقاية من الهجمات السيبرانية الممكنة ، و قد ظهرت العديد من الإستراتيجيات و لعل نظرية الردع أهمها ، و تسعى هذه الدراسة في التفصيل في هذه الإستراتيجية و التطرق لمحاورها و مدى ملامتها للواقع السيبراني الذي يختلف تماما عن المجال العسكري و غيره من المجالات التي تطبق فيه هذه الإستراتيجية .

الكلمات المفتاحية:

الإستراتيجية ;الاستبقاية ; أمن المعلومات ; السيبرانية ، الردع .

Abstract:

In the wake of the events of September 11, 2001, the United States of America found itself facing new threats of a higher level than during the Cold War. It is not about confronting a similar party, but groups that are not subject to any authority or even other threats that have not been committed before. The importance of preventive methods, especially when it comes to changing and evolving threats such as cyberspace, which has become one of the most important aspects of human life and one of the basic tools in the strategies of countries

.There is no doubt that information security is one of the red lines that affect national security because it has a network link with the vital sectors of the state, which requires the existence of proactive strategies to prevent possible cyber attacks, and there have emerged many strategies and perhaps the theory of deterrence is the most important, Detailing this strategy and addressing its aspects and the extent of its relevance to cyber reality, which is completely different from the military field and other areas in which this strategy is applied.

Key words:

Strategy ; Prediction ;Information Security ; Cyber ;Deterrence .

مقدمة :

إبان الحرب الباردة لم تكن طموحات الدول إلا انعكاس لرغبة ملحة في الأمن الذاتي بأقل الخسائر ، فربما هواجس التفكك و الزوال كانت و لا تزال لصيقة التفاعل الدولي بكل أشكاله ، فلما كانت سياسة البروباغندا العسكرية أحد وسائل المنع كان السباق نحو التسلح هدفا ، ففكرة التهديد و الوعيد لم تكن يوما وليدة الصدف و لا عقيدة ذاتية بل أسلوب بشري ينعكس على مستوى الدول ، و ما عمليات الردع إلا أحد أنواع هذه الأساليب ، و بانتقال الوسائل تنتقل الأهداف وجوبا وتلازما ، فاليوم الحديث لم يعد عن ما تمتلكه الدولة من عدة و عتاد في حرب مماثلة ليتعدى لما بعده ، فما القول بأن كل ما تستخدمه الدولة في حماية أمنها قد يشكل خطر عليها إلا إشارة واضحة لجدلية الأمن و الخطر فمواطن الدولة ذاتها قد يكون تهديدا لها ، و قد يكون الخطر في ما تتبناه في خطط سياسية أو اقتصادية أو تنوع هوياتي و غيره و الكل يتأرجح بين الحالتين فلهذا فإن تنامي المجال السيبراني واستخداماته أصبح يطرح عدة إشكالات أمنية .

أهمية الدراسة :

تتضح معامل التساؤل في الدراسة في أن واقع التهديدات الحالية أصبح أكثر تعقيدا باتساع مطالب الأمن ، و عند الحديث عن ذات المطالب فإنها مرتبطة بحركية الفواعل فيها و التي هي مجال أوسع بالأخص في الفضاء السيبراني الذي يضم فواعل متعددة من جهات رسمية و غيرها ، فإن عملية التهديد تبدو أكثر سهولة في ظل شيوع استخدام هذا النوع من التكنولوجيا ، و هنا يبرز دور الإستراتيجيات الحمائية و فعاليتها في مواجهة الأخطار اللاتماثلية الجديدة .

أهداف الدراسة :

تهدف الدراسة لتوضيح أهم المفاهيم المتعلقة بالدراسة كمطلب أولي ، إذ أن كل من الفضاء الإلكتروني و التشابك المعلوماتي و كذا العلاقة بينها و بين المفاهيم الأمنية تحوم حولها بعض الغموض في ظل حداثة الظاهرة المتعلقة و روابطها ، و يضاف لذلك تحديد واقع نقل الإستراتيجيات الإستباقية لهذا المجال و تقييم فعاليتها في صورة دراسة أنموذج الردع و متطلباته .

إشكالية الدراسة :

تأسيسا لما سبق فإن الموضوع لا يزال يثير عدة تساؤلات تدور أغلبها في مدى نجاعة نقل الإستراتيجيات الإستباقية في مجال أمن المعلومات ، و يتم طرح الإشكالية كالآتي :

- ما مدى مساهمة آلية الردع السيبراني كأحد الأساليب الإستباقية في تحقيق الأمن المعلوماتي في ظل حالة فوضى الفواعل في العالم السيبراني ؟.

تفترض الدراسة مبدئيا أنه كلما اتّسمت الإستراتيجيات الإستباقية بالمرونة كلما تجاوبت مع الهجمات السيبرانية المتغيرة بتغير الفواعل .

منهجية الدراسة :

يتم الإعتماد في الدراسة على المنهج التفكيكي التركيبي بحيث تم تفكيك محاور الدراسة و إعادة تركيبها بما تناسب مع طبيعة الموضوع ، بالإعتماد على تقنية تحديد الحالة من منهج دراسة الحالة عبر التطرق لإستراتيجية الردع كأنموذج ، بالإضافة لتقنيات التحليل و الوصف في عدة مواضع في الدراسة .

المبحث الأول

الربط المفاهيمي بين أمن الفضاء السيبراني و الإستباق

المطلب الأول : تحديد مفهوم الأمن السيبراني.

يعتبر مصطلح الأمن السيبراني مفهوم جديد نوعا ما فقد ارتبط ظهوره بالثورة التكنولوجية التي عرفها البشر، ومع تزايد اعتماد الإنسان على وسائل التكنولوجيا و الإتّصال وما واكبها من تحديات كبرى، و لعل أهمها مجابهة ما يطلق عليه اسم الفضاء السيبراني الذي يتم اعتباره على أنه مجال افتراضي لنظم الكومبيوتر و شبكات الإنترنت، وقد ظهر كمصطلح في ثمانينيات القرن الماضي في إحدى روايات الخيال العلمي للكاتب الأمريكي ويليام جيبسون، والذي تم وصفه على أنه العصر الرقمي المتصف بالتطورات التكنولوجية و انعكاساتها على المجتمع الدولي ، و تم التنبؤ على أنه مستقبل الحضارة الإنسانية و أساس التواصل و هو ما حصل فعليا من خلال تطورات الوقت الحالي[1].

واختلفت التعريفات حول هذا المصطلح باختلاف طبيعة الدول، وكذا الإستراتيجية التي تعتمدها و مدى إرتباطها بالعالم الرقمي، والتي ترتبط بمدى تفعيل الحكومة للنظم الإلكترونية و توظيف شبكات المعلومات و وسائل الإتصال السلكية و اللاسلكية، وبالطبع توصيل الخدمات للمواطنين في مجالها المدني من جهة، واستخدام هذه التكنولوجيا في المجالات العسكرية وإستراتيجيات الدفاع من جهة أخرى [2]، وعموما يعرف على أنه عالم افتراضي يتشابك مع العالم المادي يتأثر و يتأثر بشكل مترابط، وتقوم هذه العلاقة على نظرة تكاملية تحمل بين طياتها مزايا ومخاطر متعددة [3].

وبالعودة لمفهوم الأمن السيبراني في مواجهة مخاطر الهجمات، فإنه إذا كان مصطلح الأمن نفسه قد توسع بدوره، فإن ما ارتبط به يجري عليه ما سبقه، وقد قدمت وزارة الدفاع الأمريكية تعريف مهم له بوصفه جميع الإجراءات التنظيمية اللازمة لحماية المعلومات بكل أشكالها في مواجهة جميع الأخطار و الهجمات ذات الصلة [4]، وتعرفها مارجريت روس (Margaret rouse) بأنها حماية الاتصال بالإنترنت بما فيها العمليات البرمجية و الأجهزة

---

[1] نورة شلوش، " القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول "، **مجلة مركز بابل للدراسات الإنسانية**، العدد 6، المجلد 8، جامعة بابل، العراق ، 2018، ص 190.

[2] سحر قدوري الرفاعي، " الحكومة الإلكترونية وسبل تطبيقها: مدخل إستراتيجي "، **مجلة اقتصاديات شمال إفريقيا**، العدد 07، جامعة حسيبة بن بوعلي، الشلف، ديسمبر 2016، ص 308.

[3] نورة شلوش، مرجع سابق، ص 190.

[4] بن مرزوق عنترة وحرشاوي محي الدين، " الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية "، **مجلة دفاتر السياسة والقانون**، العدد 17، جامعة قاصدي مرباح، ورقلة، جويلية 2017 ، ص 66 .

الضامنة لها، وكذا البيانات من الهجمات السيبرانية (cyberattacks).[1]، ولعل ما يشير له التعريفين هو حالة الأمن الناتجة عن غياب الخوف من الهجمات الإلكترونية المهددة لسير العملية الإتصالية التي تقوم بها الأطراف الرسمية وغير الرسمية، وقد تتضمن هذه العملية الإجراءات العادية أو الخاصة بما يعكس طبيعة الصراع القائمة.

أما كل من (مارتي ليهتو) و (بيكا نيتانمكي) (MarttiLehto)&(PekkaNeittaanmäki)فيقدمان تعريف محدد في كتابهما بعنوان " الأمن السيبراني، التحليل والتكنولوجيا "، بحيث يعتبر مجموعة الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكومبيوتر و عواقبها، وبما يضمن تنفيذ التدابير والإجراءات المضادة للحماية [2].

من خلال هذه تعاريف يمكن القول بأن الأمن السيبراني كمفهوم تزامن مع ظهور الثورة في تكنولوجيا المعلومات والاتصال، ويرمز في دلالاته للقدرة على مجابهة الهجمات الإلكترونية، ومختلف التهديدات ذات الصلة و التي تقوم بها جماعات أو دول أو أفراد، وبالنظر لأهمية المعلومات لدى الدول في الوقت الحالي، فإن مسألة حمايتها تعد من الأولويات التي يتم استنفار كل الموارد لإدراكها .

المطلب الثاني : مفهوم الهجمات السيبرانية.

أولا . تعريف الهجمات السيبرانية:

تعرف الهجمات السيبرانية على أنها فعل يقوض من قدرات وظائف الشبكة المعلوماتية من خلال استغلال أحد نقاط الضعف ما يمنح المهاجم القدرة على التلاعب بالنظام[3]، أما جونيدو مارشال (junaidu Marshall) فيعرفها على أنها عملية الاستغلال المتعمد لأنظمة الكومبيوتر والشبكات المعتمدة على التكنولوجيا من خلال البرمجيات الضارة [4]، وتتعدد ما بين الأساليب الممنهجة أو العشوائية فقد تستخدم من طرف الرسميين كأساليب ضغط أو بشكل عشوائي من طرف محترفيين للنفع الذاتي أو هجمات منظمة من طرف جماعات مارقة.

ثانيا . أنواع الهجمات السيبرانية:

تتخذ الهجمات الإلكترونية عدة أشكال تساهم في اختراق الأنظمة الدفاعية و البيانات من خلال استغلال نقاط الضعف ، و يمكن تحديد أهمها في:

- سرقة كلمات المرور والتسلسل للنظام: وتتمثل في التخمين والخداع والبرمجيات الخبيثة والنفاذ لملف تخزين كلمات المرور.

[1]Margaret rouse, Cybersecurity , **search security** , Network security , link seen in 10/02/2019 : https://searchsecurity.techtarget.com/definition/cybersecurity

[2]بن مرزوق عنترة وحرشاوي محي الدين، مرجع سابق، ص 66 .

[3]نورة شلوش، **مرجع سابق**، ص 191.

[4]Junaidu Bello Marshall , Cyber attacks : the legal response **, International journal of international law** , Vol 01 , Is 02 , universal multidisciplinary research institute , india , P 03 .

- هجمات رفض أداء الخدمة: وهي هجمات إنكار الخدمة " هجمات دوس (DDOS) تستخدم لزيادة التحميل على الإنترنت مما يؤدي للضغط على الشبكات ويمنع المستخدمين من الوصول للمنتجات والخدمات، ويعتمد هذا النوع من الهجمات على نوعين من الروبوتات هي :

أ . القائم على الاتصال: وتحدث عندما يكون هناك تبادل بين الخادم و العميل باستخدام طرق معينة.
ب . منقطع الاتصال: وتقوم بالأساس على عامل تغيير الاتصال أو انقطاعها والتسلل بين هذه العقبات.
ج . الهجمات الطمسية: وتعتمد على طرق استبدال الصفحات بغيرها بهدف الشك والتقلب.
د . هجمات البنية التحتية: وتستهدف شبكات الكهرباء والاتصالات والأغذية والصرافة والمالية.
ه .قرصنة المعلومات: وتتمثل في سرقة بيانات معلوماتية وسرقة حقوق الملكية أو تهكير حقوق التأليف، وينشط في هذا المجال إما المحترفون وهم الذين يستخدمون تقنيات في محاولات الاختراق والحصول على معلومات سرية أو التخريب، أما الهواة فهم أخطر أنواع الهاكرز الذين يتسللون عبر الشبكات الهاتفية والتقنيات غير القانونية مما يصعب عملية التعقب [1].

المطلب الثالث : الإستباقية والوقائية، التلازم الاصطلاحي.

كثيرا ما يترادف مصطلحي الاستباق والوقاية في سياق وضع خطط ذات المدى الطويل و المتوسط، ويرمز للمصطلحين في اللغة العربية بدلالتين قريبتي المعنى إذ أن الوقاية تعني الحماية من الأخطار القادمة، أما الاستباق فهو توقع خطوات أو سيناريوهات قادمة لوضع حلول لها إذا فالاستباق خطوة تسبق الوقاية .

أما في اللغة الإنجليزية فيبرز مصطلح (Preventive) المشتق من الفعل اللاتيني (Praevenire) الذي يقصد به منع شيئ ما من الحدوث، وقد ورد في قاموس أوكسفورد أن الاستباق هو الأمل لفعل شيئ يمنع حدث معين من الوقوع أو التحضير له [2].

وعلى المستوى الاصطلاحي فإنه تجدر الإشارة أن ظهور المصطلحين تزامن مع تطور الفكر الإستراتيجي الأمريكي على الرغم من أن الكثير من الدارسين يرجعون المصطلح لما بعد 2001 م إثر هجمات 11 سبتمبر ، و تبلور هذا المصطلح بالتزامن مع العقيدة الأمنية الأمريكية في فترة الحرب الباردة وما بعدها وفق إستراتيجيات قائمة على التوقع و الوقاية مثل الاحتواء والردع.

وتأسيسا لذلك فإن أغلب التعاريف للمصطلح ترتبط بالمفاهيم الأمنية العسكرية بالأخص، إذ يوجد مصطلح الحرب الوقائية وهو نوع من الحروب الهجومية دون الرد على هجوم مماثل بما يرمز لاستخدام القوة كأداة دفاعية، أو بمعنى آخر عملية افتراض وجود خطر محدق و السعي لدفعه، وعليه يفترض إسماعيل صبري

[1] نورة شلوش، **مرجع سابق**، ص 191.

[2] بن عمار إمام، " الحروب الوقائية في الفكر الإستراتيجي الأمريكي – دراسة حالة العراق – "، **مذكرة ماجستير**، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2008، ص 17.

مقلد أن الحرب الوقائية تعتبر المظهر الرئيسي للتخطيط الإستراتيجي على الأساس الهجومي، بحيث يسعى كل طرف معين لتبني إستراتيجية معينة تضمن له الأسبقية [1].

وبالتطرق للمعنى القانوني للمصطلح فإنها تشير لمجموعة من التدابير الوقائية إذ يتم إضفاء الطابع القانوني عليها، وهي عملية وضع تشريعات تمنع فرد معين أو جماعات من ارتكاب فعل غير قانوني يتم تحديده من طرف المشرع لمواجهة الخطر الإجرامي [2].

وعموما يمكن القول أن مصطلح الإستباقية أو الوقائية يتميز بنوع من المطاطية، بحيث أنه علميا يعد أحد مصطلحات الاستشراف القديم نوعا ما، أما عمليا فإن بداياته كانت في المجال الأمني تحديدا إلا أنه انتقل للمجالات الأخرى، فيمكن ملاحظة الإستباقية الاقتصادية أو الوقائية القانونية و غيرها من المجالات التي إستفادت من تطور التقنية و المصطلح، وعليه فإن ظهوره في مجال الأمن السيبراني ليس بغريب كونه أحد المجالات المرتبطة بالأمن في الوقت الحالي الذي هو المجال الحيوي للمصطلح بالأساس، وهو ما عجل بظهور مجموعة الإستراتيجيات الإستباقية في ذات المجال سيتم التطرق لها في العناصر الموالية.

المطلب الرابع : السيبرانية بين خطر الهجمات العشوائية واستباق الإجراءات.

تتعلق أغلب مضامين الصراعات الحالية بمدى الاستخدام المتعدد لوسائل الاتصال والذي يرتبط بعاملي الاستغلال الحيوي والمظلة الأمنية للحماية ضد الهجمات الخارجية حيث تعني في أحد دلالاتها قيام فاعل أو مجموعة فواعل رسمية وغير رسمية بشن هجوم إلكتروني، وهو ما يجسد ما يسمى بالحروب السيبرانية في ظل تمدد الأعمال العدائية في إطار الحرب غير المتكافئة، وذلك لكون الطرف الذي يتمتع بقوة هجومية بغض النظر عن حجم القوة العسكرية هو من يستطيع التأثير في الطرف الآخر، ويتوقف توظيف المصطلحات لوصف هذه الهجمات على مدى الاستغلال السياسي للهجمات إذ قد تعد عملا إرهابيا أو قرصنة إلكترونية[3]، وهو ما يتطلب وجود بناء حقيقي لمجابهة هذه الأخطار من خلال مجموعة من العناصر الأساسية و المتمثلة في:

أولا . متطلبات القوة السيبرانية:

وهي القدرة على التأثير من خلال استخدام وسائل الاتصال و شبكاته وغيره من العناصر والمتطلبات، والتي تتمثل في التالي:

أ . البنية التكنولوجية:

---

[1] صالح ياسر، " من إستراتيجية الردع والاحتواء إلى إستراتيجية " الهجوم الوقائي "، تحول خطير في التفكير الإستراتيجي الأمريكي بعد 11 أيلول / سبتمبر 2001 "، **مجلة الحزب الشيوعي العراقي** ، المصدر اطلع عليه في 2019/02/10 :
http://www.iraqicp.com/images/pdf/yaser14.pdf

[2] أسعد عبد الحميد إبراهيم ، " التدابير الوقائية في القانون الجنائي "، **مجلة جامعة شندي** ، العدد 04، جامعة شندي، السودان، 2007، ص 02 .

[3] عادل عبد الصادق، " أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي "، **مجلة السياسة الدولية**، نشر في 2017/05/14، تم الإطلاع على المصدر في 2019/02/10:
http://www.siyassa.org.eg/News/12072.aspx

إذ تحتاج الدولة لأجهزة ذات كفاءة عالية و شبكات اتصال متعددة، وكذا برمجيات متطورة بالاعتماد على خبرة العنصر البشري المدرب من أجل البنية التحتية للقوة السيبرانية، وتستطيع الدولة من خلالها التأثير على الإقليم باستخدام القدرات الإلكترونية من جهة، وتأمين نفسها من الأخطار الممكنة من جهة أخرى .

ب . الفيروسات والبرامج الخبيثة:

وهي برامج تصميم من أجل تنفيذ عمليات قرصنة مثل الإزالة أو التعديل أو التخريب بغرض التأثير على أجهزة الدول الأخرى، وتستخدم لعمليات تعطيل شبكات البنية التحتية و كذا تحويل عمليات الاتصال وسرقة المعلومات .

ج. القدرة على القيام بالعمليات الإلكترونية:

والتي تضمن عمليات اختراق الشبكات ومهاجمة أنظمة المعلومات و تدعى بالقدرة الهجومية، أما القدرة الدفاعية فهي تحتوي على عمليات الحماية من الهجمات المختلفة، وإمكانيات تشغيل الأجهزة ببرمجيات معينة، أما القدرة الاستطلاعية فهي عملية الدخول للحواسب والتجسس على الشبكات المحلية وخطط الدفاع، والقيام بالعمليات الإستخبارتية المختلفة بغرض معرفة خطوات الخصم [1].

إن القوة السيبرانية تتطلب توفير أقصى درجات الأمن الإلكتروني، وذلك من خلال تبني سياسات دفاعية تتضمن عمليات الحماية والتطوير لإجراء الدفاع ضد الأخطار المحتملة، والتي تتعلق بحماية نظم المعلومات و منع تعرضها للهجمات المعادية، ويبرز نمطين أساسيين للقوة السيبرانية تتمثل في:

نمط القوة الصلبة:

وهي استخدام المقدرات والأدوات في عمل تخريبي عبر قطع كابلات الاتصالات أو تدمير أنظمة الاتصالات أو الأقمار الصناعية، وحتى استعمال البرامج التخريبية و تنفيذ عمليات سرقة منظمة للبيانات.

نمط القوة الناعمة:

وهو عملية استخدام القدرات السيبرانية في جانب التأثير الناعم على الطرف الآخر، وفق نظريات التشويش وتغيير مسارات القوة عبر التلاعب بالمعلومات وتوظيف نتائجها لخدمة المصالح المستهدفة [2].

ثانيا. أنواع الإستراتيجيات الإستباقية في الفضاء السيبراني.

تتعدد الأساليب و الطرق الإستباقية والتي بدورها تساهم في التصدي للهجمات السيبرانية، وتختلف في مفاهيمها باختلاف أطرافها أو ظروفها أو طبيعتها و تتمثل في صنفين أساسيين هما:

أ. الإستراتيجيات الهجومية:

---

[1] نسرين الشحات الصباحي، " الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول، دراسة حالة إسرائيل منذ 2010 "، **المركز العربي الديمقراطي**، برلين، نشر في 2016/04/29، المصدر أطلع عليه في 2019/02/10:

https://democraticac.de/?p=30962

[2] عادل عبد الصادق، " الفضاء الإلكتروني وأسلحة الانتشار الشامل بين الردع و سباق التسلح "، **مؤتمر حروب الفضاء السيبراني**، نشر في 2015/05/15، المصدر اطلع عليه في 2019/02/11:

https://seconf.wordpress.com/2015/05/15/%D8%

وهي تلك الطرق التي يتم استخدامها ضد أطراف معينة قد تشكل خطر مستقبلي على بيانتها، وتعتمد بالأساس على عملية إطلاق ديدان إلكترونية أو فيروسات أو أي نوع آخر من الهجمات السيبرانية، ولعل أشهرها ما يسمى بحصان طروادة التي تعتمد على حزمة الفيروسات الخفية التي تهاجم الخصم بشكل فجائي و طريقة الأبواب الخلفية المعتمدة على استغلال ثغرات نظام العدو و إستراتيجية حجب الخدمة، وتهدف كلها شل طرف معين أو زعزعة قدراته الهجومية [1].

ب. الإستراتيجية الدفاعية:

وتتمثل في مجموعة الإجراءات الدفاعية التي تتمثل في تطوير الذات وتقوية القدرات لمواجهة الأخطار الممكنة، وتتركز أغلبها في تجهيز مجموعة من الأنظمة ذات أبعاد مختلفة تتمثل في:

البعد العسكري: وهي عملية الحماية الأمنية للمعلومات من خلال بلورة أنظمة للدفاع السيبراني، وغالبا ما تكون هذه الأنظمة والإستراتيجيات ذات مستوى عالي من السرية .

البعد الاجتماعي: وهي عملية تأمين البيانات للأفراد و تختلف ما بين أساليب الردع القانوني مثل إجراءات ردعية لمعاقبة المخترقين للحسابات الشخصية وسرقة الملكية المعلوماتية و غيرها والردع المعلوماتي المتمثل في إنشاء أنظمة الحماية ونشر التوعية الاجتماعية حول الاستخدام الآمن.

البعد السياسي: وهو امتلاك الدولة الحق في حماية نظامها السياسي ومصالحها ومصالح مواطنيها، وذلك من خلال اعتماد إستراتيجيات داخلية متمثلة في إجراءات محلية أو خارجية من خلال العمل على التوافق الدولي لحماية الأمن السيبراني [2].

المبحث الثاني

الترسانة الجديدة للردع السيبراني، الحماية أم الانتقام

المطلب الأول : تحولات مفهوم الردع مابين المنع الصلب و الناعم.

إن الردع كمفهوم ينصب في جملة الاستعمالات التي نشأ عنها، ويشير المصطلح في اللغة العربية إلى عملية المنع القسري للفعل، فيقال " ردع " و " ارتدع " أي منع و كف و قطع، وهو ما يدل على عملية الكف ضد طرف معين من فعل شيء ما [3].

أما في اللغة الإنجليزية فيبرز مصطلح (Deterrence) ويعني عمليا منع فعل من الحصول، وذلك بناءا على مخاوف و شكوك من النتائج [4]، وغالبا ما يشير المصطلح لوجهين للردع هما العقاب والمنع فيدل الأول على عملية

---

[1] محمد الدوراني، " قتال غير مرئي: الحرب السيبرانية في الأزمة الخليجية "، **تقرير مركز الجزيرة للدراسات**، نشر في 2018/05/13، اطلع عليه في 2019/07/07:

http://studies.aljazeera.net/mritems/Documents/2018/5/15/

[2] يوسف بوغرارة، " الأمن السيبراني: الإستراتيجية الجزائرية للأمن و الدفاع في الفضاء السيبراني "، **مجلة الدراسات الإفريقية و حوض النيل** ، المجلد 01 ، العدد 03 ، المركز العربي الديموقراطي ، برلين ، سبتمبر 2018 ، ص 108 .

[3] عبلة مزوزي، " إستراتيجية الردع وانعكاساتها على الواقع الإقليمي والدولي بعد نهاية الحرب الباردة – دراسة حالة إيران – "**أطروحة مقدمة لنيل شهادة الدكتوراه**، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2018، ص 17.

[4] Definition of deterrence in English ,**Oxford dictionaries** , link 12/02/2019 :

شل قدرة الطرف الآخر على الهجوم أو رد الفعل انطلاقا من مخاوف، أما المنع هو عملية التحضير للدفاع عبر جملة الإجراءات المضبوطة [1].

صحيح أن مفهوم الردع بدأ علميا و عمليا في المجال العسكري، والذي ينطلق من الردع العسكري بامتلاك الأسلحة اللازمة، وقد شاع إبان الحرب الباردة وارتبط أساسا في فترة الحرب الباردة إلى سادتها صراعات متعددة الأشكال، ولا يشير بالضرورة للردع النووي إذ يلاحظ وجود أصول للردع كلاسيكيا تاريخيا إذ ساد في العصر الروماني بوجود خطط هجوم اعتمدها الرومان لحماية أمنهم خارج حدود الإمبراطورية، وبالحديث عن الردع النووي فإنه ضمنيا يرتبط بوجود ترسانة من الأسلحة تمنع أي طرف من الهجوم [2]، و من هذا يمكن إيجاد تعريف للردع في الزمن الحاضر المعبر عن حسابات جديدة للقوة و الردع تزامنا مع تغير مفهوم الحروب التقليدية لمفهوم جديد، فالأمر يتعدى ساحات القتال للحروب ذات قيم مادية ومعنوية التي قد تنشب بين دولتين أو مجموعة دول أو بين دولة وجماعة مدنية وعسكرية أو حتى بين دولة وبضعة أفراد، مما تطلب وجود مفاهيم جديدة للردع بعيدا عن المفاهيم التقليدية [3].

ويعرف الردع السيبراني على أنه منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والتي تدعم العمليات الفضائية، ولعل أقرب ما يمكن قوله عن الردع السيبراني يلخصه الجنرال الأمريكي كارتيرايت (Catwright) في حدود قوله التالي: " إننا بحاجة لتطوير قدراتنا في الفضاء السيبراني لمواجهة ماقد يريد الآخرين فعله اتجاهنا "، وهو ما يعكس منطق الردع الذي يشير للقدرة على الفعل قبل رد الفعل بإستجابة تشابه الإستجابة التقليدية، ويمكن تمييز نوعين من الردع فقد يعني الانتقام من جهة و المنع من جهة أخرى.

وهناك من يعتقد أن السيطرة على الفضاء السيبراني يتقدم الردع لتجنب التصعيد وأن استخدام القوى المادية يمثل انتقامًا عينيًا على استخدام الهجمات الإلكترونية، وهناك من يجد أن الانتقام العيني أكثر جاذبية من البدائل الأكثر عنفاً لأن الأول يثير عددًا أقل من قضايا التناسب. وعلى العكس من ذلك فإن الانتقام العيني يمكن أن يضفي شرعية على شكل من أشكال الحرب، بحيث لا يكون من مصلحة الطرف الأقوى إضفاء الشرعية عليها عندما يكون لديه أكثر من قوة تقليدية ملائمة لكل مناسبة [4].

المطلب الثاني : مرتكزات الردع السيبراني.

يمكن القول أن عملية الردع السيراني كغيرها من الإستراتيجيات المماثلة تستند لمجموعة من المرتكزات يتم تصنيفها في نقاط أساسية تتمثل في:

---

https://en.oxforddictionaries.com/definition/deterrence

[1] Martin C .Libicki , Expectations of cyber deterrence **,Strategic studies quarterly** , 2018 , Link 13/02/2019 :
https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-4/Libicki.pdf

[2] بجيح زيدان، " سياسة الردع النووي بين توفير الأمن والسلم الدوليين والهيمنة "، **مذكرة ماستر**، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2017، ص 06 .

[3] عبد الجليل زيد المرهون، " عصر الردع الإلكتروني "، **موقع الجزيرة**، نشر في 2009/05/02، اطلع عليه في 2019/02/14:
https://www.aljazeera.net/knowledgegate/opinions/2012/

[4] Martin C libicki**,Cyberdeterrence&cyberwar** ,(USA : Rand corporation , 2009) , P 27 .

أ. **الردع من حيث النوع:**

يمكن تمييز نوعين من الردع إذ يشير الأول لعملية الردع بالمنع، والذي ينطوي تحته ما يسمى بالردع بالمقاومة وهو مقاومة الهجمات الإلكترونية ومنعها من تحقيق أهدافها، أما الردع بالصمود يعني القدرة على استعادة الشيء بشكله الأصلي قبل الهجوم مما من شأنه أن يحد من المكاسب المحتملة، أما عملية الانتقام فتعني عملية الرد على الهجمات التي حدثت بالفعل بما يتناسب مع الخسائر ماديا و معنويا [1].

ب . الردع من حيث الفعل:

يستند حدود الفعل في الردع في ثلاثة ركائز أساسية، حيث تتمثل الأولى في مصداقية الدفاع عن أنظمة المعلومات ومنع أي محاولات لاختراقها عبر توافر أنظمة نسخ احتياطية (Backup Systems)، مما يعني أن أي هجوم في هذه الحالة لن يسفر عن التدمير الكلي في ظل إمكانيات الاستعادة الذاتية، أما الركيزة الثانية فتتمثل في القدرة على الانتقام التي تتطلب وجود آليات للرد على الهجمات، ما يمنح الطرف المتعرض للهجوم القدرة على إعادة بناء الذات وتحقيق التوازن مع الطرف المهاجم، أما العنصر الثالث فهو عملية الرغبة في الرد أي وجود نوايا للرد مع وجود القدرة على القيام بالفعل [2].

ج . الردع من حيث المتطلبات:

يتم تمييز مجموعة من الأساليب لضمان عملية الردع السيبيراني في شكل خيارات وإجراءات تتخذ في مواجهة الهجمات الممكنة تتمثل في:

الردع السلبي:

وهو عملية عدم الرد على الهجمات أو تهديدات اللجوء إليها، لكن مع الاعتراف بأن مسألة أمن المعلومات والإجراءات المتعلقة بها لا تزال غير كافة، ومنه فإن عملية التطوير قد تمنع وقوع الهجمات المستقبلية [3].

الإجراء الدبلوماسية والقانونية:

وهي عبارة عن مجموعة الخطوات الدبلوماسية والقانونية، إذ يتم اعتماد الاستجابة الرمزية ضد الطرف المهاجم بطرد البعثة الدبلوماسية أو بعض أفرادها، مما قد يسبب زعزعة مكانة الطرف المعتدي دوليا، أما الإجراءات القانونية فتتمثل في توجيه الاتهامات ضد الأفراد و المنظمات المضطلعة في الهجوم السيبراني ولو

---

[1] عبد الغفار الديواني، " القرن السيبراني: الردع الإلكتروني بين المنع والانتقام "، **مجلة المستقبل للأبحاث و الدراسات المتقدمة**، المعهد الألماني للشؤون الدولية والأمنية، نشر في 2015/06/04، اطلع عليه في 2019/02/14:

https://futureuae.com/ar-us/Mainpage/Item

[2] رغدة البهي، " الردع السيبراني: المفهوم والإشكاليات والمتطلبات "، **مجلة العلوم السياسية والقانون**، العدد 01، المركز العربي الديموقراطي، برلين، جانفي 2016، ص 52.

[3] نفس المرجع السابق، ص 59.

كانوا مسؤولين حكوميين، وبالطبع فإن هذا الإجراء لابد أن يتضمن أدلة دامغة لاستخراج مذكرة دولية للإعتقال، وإلا سيبقى رهين التهديدات الجوفاء[1].

العقوبات الاقتصادية:

وهي عملية فرض إجراءات اقتصادية ضد الأطراف المعتدية من عقوبات مالية و فرض غرامات ضد أفراد بعينهم أو الجماعات، أو حتى حظر التعامل الاقتصادي و التبادلات بكل أنواعها [2].

الأعمال الانتقامية:

والتي تعني عملية فرض هجمات انتقامية سيبرانية سواء برد الفعل بنفس عملية الاعتداء، أو تجاوز الحد المطلوب من خلال الاتجاه للهجوم المسبق كغطاء لعملية متوقعة، وقد تتجاوز الانتقام في المجال الفضائي إلى مجالات أخرى أكثر قوة مثل المجال العسكري الذي يفترض وجود ضربات عسكرية بغرض الانتقام [3].

د . الردع من حيث المرونة:

حيث يختلف الردع التقليدي على الردع السيبراني من حيث مرونة الرد أو الاستجابة للهجمات الممكنة أو الموجودة فعليا و التي تتضح في طريقتين:

وجود الأنظمة البديلة:

والتي تفترض اعتماد مجموعة من البدائل التي تضمن استمرارية المعلومات في حالة التعرض لهجوم سيبراني، ويمكن لأي طرف خلق أنظمة بديلة في حوزة الأطراف نفسها أو أطراف أخرى.

عملية إعادة التأسيس:

وهي عملية إعادة بناء النظام المخرب بسرعة و إعادة تشغيل النظام، ولكن الطريقة الوحيدة لتجنب الهجوم هي الاحتجاب عن الجميع، وخلق نوع من الاستقرار والتمويه المعلوماتي لتجنب الضربة المباشرة، أو توزيع المعلومات لضمان عدم خسارتها كلها [4].

المطلب الثالث : تحديات الردع السيبراني.

إن متطلبات الردع السيبراني لا تزال غير كافية رغم وجود تحديات حقيقية، إذ لا تزال مشكلة تحديد الجاني تؤرق الكثير خاصة وأن الواقع المعلوماتي يشير إلى أن الفضاء السيبراني مفتوح وواسع ولا يقتصر على الأطراف الرسمية وكذا غياب آليات إلزامية لمعاقبة الأطراف المعتدية مما يجعل الردع أشبه بالعمليات العشوائية الانتقامية .

---

[1] Sico van der meer&franspaul van der putten , US deterrence against chinese cyber espoinage, **policy brief** , clingendael , netherlands institute of international relations , september 2015 , P 04 . link seen in 15/02/2019 :
https://www.clingendael.org/sites/default/files/pdfs/

[2] رغدة البهي، مرجع سابق، ص 60.

[3] Sico van der meer&franspaul van der putten, op cit, P 05.

[4] رغدة البهي، مرجع سابق، ص 61.

وفي هذا الصدد اقترحت روسيا عام 1999 إنشاء معاهدة دولية لحظر الأسلحة الإلكترونية، وتم طرح ذات الموضوع مع الصين في منظمة شنغهاي للتعاون، وكذا الاتفاق في 2003 م في الأمم المتحدة التي تقضي بتعيين خبراء حكوميين دوليين للحد من الصراع وتشكيل قواعد معيارية بين الدول ذات التفكير المتشابه، يضاف لذلك بناء معايير أمنية مشتركة بين القطاع العام والخاص لإنشاء مدونات لقواعد السلوك [1].

ولعل أبرز مشكل قد يواجه إستراتيجية الردع العالمية هو مسألة المرونة في ظل الروابط الضيقة بين الأطراف ما من شأن المعاهدة أن تضر بنوعية المرونة، وحتى مسألة المنع الذي قد تخضع لحسابات التكلفة خاصة في ظل وجود فوارق في التفوق التكنولوجي، ويضاف لذلك مشاكل عملية الانتقام التي قد تؤدي لكشف معلومات ضرورية على البنية الدفاعية السيبرانية، ما قد يفتح الباب أمام هجمات متطورة في المستقبل تتجاوز القدرات الموجودة فعليا، وهذا ما يقوم به الهاكرز الذين يستفيدون من نقاط الضعف التي تظهر في عملية الدفاع الأولية ضد الهجوم [2].

خاتمة:

يمثل الاستباق عامل مهم في العلاقات الدولية فكثيرا ما تسعى الدول لتبني منطلقات وقائية لحماية نفسها من الأخطار الممكنة، وهذا مرتبط بالأساس بالشكوك و الهواجس التي ترادفت مع بناء الدول، ولعل النجاح النسبي لهذه الإستراتيجيات ساهم في محاولة نقلها للمجالات الأخرى، ويعد المجال الأمني فضاء خصبا لتجريب هذا النوع ، وبالانتقال للمجال السيبراني فإن هذه الإستراتيجيات تعد الأنسب لوجود خصوصيات تتمثل بالأساس بفجائية التهديد في ظل صعوبة تحديد إطار للأخطار القادمة.

وبالحديث عن أهمية الإستراتيجيات الوقائية فيعد الردع من بين أكثر الإستراتيجيات أهمية وأقدمها استعمالا، فعمليا يمكن ملاحظتها في السلوك الإنساني بالانتقال للإمبراطوريات القديمة أين تم الاعتماد على الاستعراضات العسكرية لما تمتلكه من وسائل قتال، فهي أحد منطلقات الردع بأبسط معانيه، ولعل فترة الحرب الباردة شهدت ثورة تنظيرية للردع ساهمت في بلورة أبرز اتجاهاته ومنطلقاته.

إن مشكلة الردع الكلاسيكي كانت متمثلة في غياب عامل المرونة، وهذا بالحديث عن المجالات العسكرية الصلبة، فإن هذا العامل قد يشكل أزمة حقيقية بالانتقال لمجالات أكثر حيوية واتساع، وهذا ما يتجسد فعليا في الفضاء السيبراني والذي يرجع بالأساس لعدة عوامل أهمها:

- **صعوبة تحديد الفاعلين:** حيث أن واقع تبادل المعلومات يعكس وجود فواعل متعددة تنشط في مجال واسع من منظمات و أفراد وجماعات.
- **إشكالية الرقابة:** تبرز مشكلة فوضى الفواعل وكذا صعوبة وضع قيود على تبادل المعلومات في مجال مفتوح و واسع، بما يفوق قدرات الدول و المنظمات على تأطير العملية عكس المجالات الأخرى التي يمكن ضبطها.

---

[1] جوزيف ناي الابن، " التحكم في الصراع السيبراني "، **موقع الجزيرة**، نشر في 2017/08/09، اطلع عليه في 2019/02/15 :
https://www.aljazeera.net/knowledgegate/opinions/2017/8/9/

[2] نسرين فوزي اللواتي، " الردع الإلكتروني، العامل الحاسم في مواجهة الخصوم "، **مجلة الأهرام الإلكتروني**، نشر في 2017/05/25، اطلع 2019/02/15:
http://aitmag.ahram.org.eg/News/77865.aspx

➢ **صعوبة الاسترجاع :** يتطلب الردع في المجال السيبراني تحديث مستمر للقدرات التقنية والمعلوماتية في ظل التطورات التكنولوجية التي يعرفها المجال السيبراني بشكل دوري، ومنها فإن عملية استرجاع البيانات وإعادة بناء الأنظمة المعلوماتية تعتبر صعبة جدا، وتتطلب إعادة تطوير الأنظمة لسد الثغرات التي يستغلها الهاكرز في الهجمات، وهو ما يستدعي بالأساس قدرات عالية قد لا تتوفر عند العديد من الدول.

تأسيسا لما سبق فإن يتم طرح عدة اقتراحات تتمثل في:

- ضرورة تشديد إجراءات الرقابة على مستعملي الفضاء الإلكتروني، والاتجاه لتقنية الرقم الخاص للاتّصال بشبكات المعلومات مما يسهل عملية الوقاية ضد الهجمات المختلفة.
- وجود تلازم في الإجراءات الردعية و عدم اقتصارها على الوسائل السيبرانية، فكل من العناصر الاقتصادية والسياسية والعسكرية تعتبر أدوات مهمة لدعم الردع الإلكتروني .
- ضرورة عصرنة أنظمة المعلومات وتطوير الاستجابة في مواجهة الهجمات الإلكترونية المتطورة .

قائمة المصادر والمراجع:

1. أسعد عبد الحميد إبراهيم، " التدابير الوقائية في القانون الجنائي "، **مجلة جامعة شندي**، العدد 04، جامعة شندي، السودان، 2007 .

2. بن مرزوق عنترة وحرشاوي محي الدين، " الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية "، **مجلة دفاتر السياسة والقانون**، العدد 17، جامعة قاصدي مرباح، ورقلة، جويلية 2017 .

3. رغدة البهي، " الردع السيبراني: المفهوم و الإشكاليات والمتطلبات "، **مجلة العلوم السياسية والقانون**، العدد 01، المركز العربي الديموقراطي، برلين، جانفي 2016 .

4. نورة شلوش، " القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول "، **مجلة مركز بابل للدراسات الإنسانية**، العدد 6، المجلد 8، جامعة بابل، العراق، 2018 .

5. سحر قدوري الرفاعي، " الحكومة الإلكترونية وسبل تطبيقها: مدخل إستراتيجي "، **مجلة اقتصاديات شمال إفريقيا**، العدد 07، جامعة حسيبة بن بوعلي، الشلف، ديسمبر 2016 .

6. يوسف بوغرارة، " الأمن السيبراني: الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني "، **مجلة الدراسات الإفريقية و حوض النيل**، المجلد 01، العدد 03، المركز العربي الديموقراطي، برلين، سبتمبر 2018، ص 108 .

7. جوزيف ناي الابن، " التحكم في الصراع السيبراني "، **موقع الجزيرة**، نشر في 2017/08/09، اطلع عليه في 2019/02/15 :
https://www.aljazeera.net/knowledgegate/opinions/2017/8/9/

8.محمد الدوراني، " قتال غير مرئي: الحرب السيبرانية في الأزمة الخليجية "، **تقرير مركز الجزيرة للدراسات**، نشر في 2018/05/13، اطلع عليه في 2019/07/07 :
http://studies.aljazeera.net/mritems/Documents/2018/5/15/5

9. نسرين فوزي اللواتي، " الردع الإلكتروني، العامل الحاسم في مواجهة الخصوم "، **مجلة الأهرام الإلكتروني**، نشر في 2017/05/25، اطلع 2019/02/15:
http://aitmag.ahram.org.eg/News/77865.aspx

10. نسرين الشحات الصباحي، " الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول، دراسة حالة إسرائيل منذ 2010 "، **المركز العربي الديموقراطي**، برلين، نشر في 2016/04/29، المصدر أطلع عليه في : 2019/02/10
https://democraticac.de/?p=30962

11. عادل عبد الصادق، " الفضاء الإلكتروني وأسلحة الانتشار الشامل بين الردع و سباق التسلح "، **مؤتمر حروب الفضاء السيبراني**، نشر في 2015/05/15، المصدر اطلع عليه في 2019/02/11 :
/ https://seconf.wordpress.com/2015/05/15/

12. عادل عبد الصادق، " أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي "، **مجلة السياسة الدولية**، نشر في 2017/05/14، تم الإطلاع على المصدر في 2019/02/10 :
http://www.siyassa.org.eg/News/12072.aspx

13. صالح ياسر، " من إستراتيجية الردع والاحتواء إلى إستراتيجية " الهجوم الوقائي "، تحول خطير في التفكير الإستراتيجي الأمريكي بعد 11 أيلول / سبتمبر 2001 "، **مجلة الحزب الشيوعي العراقي**، المصدر اطلع عليه في : 2019/02/10
http://www.iraqicp.com/images/pdf/yaser14.pdf

14. عبد الغفار الديواني، " القرن السيبراني: الردع الإلكتروني بين المنع والانتقام "، **مجلة المستقبل للأبحاث والدراسات المتقدمة**، المعهد الألماني للشؤون الدولية والأمنية، نشر في 2015/06/04، اطلع عليه في :2019/02/14
https://futureuae.com/ar-us/Mainpage/Item/733/

15.عبد الجليل زيد المرهون، " عصر الردع الإلكتروني "، **موقع الجزيرة**، نشر في 2009/05/02، اطلع عليه في : 2019/02/14
https://www.aljazeera.net/knowledgegate/opinions/2012/10/26/

16. بجيح زيدان، " سياسة الردع النووي بين توفير الأمن والسلم الدوليين والهيمنة "، **مذكرة ماستر**، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2017 .

17. بن عمار إمام، " الحروب الوقائية في الفكر الإستراتيجي الأمريكي – دراسة حالة العراق – "، **مذكرة ماجستير**، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2008 .

18.عبلة مزوزي، " إستراتيجية الردع وانعكاساتها على الواقع الإقليمي والدولي بعد نهاية الحرب الباردة – دراسة حالة إيران – "، **أطروحة مقدمة لنيل شهادة الدكتوراه**، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2018 .

19. Martin C libicki,**Cyberdeterrence&cyberwar** ,(USA : Rand corporation , 2009)

20.Definition of deterrence in English , **Oxford dictionaries** , link 12/02/2019 **:**

https://en.oxforddictionaries.com/definition/deterrence

21.Martin C . Libicki , Expectations of cyber deterrence **,Strategic studies quarterly** , 2018 , Link 13/02/2019 :
https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-4/Libicki.pdf

22.Margaret rouse,Cybersecurity , search security , Network security , link seen in 10/02/2019 : https://searchsecurity.techtarget.com/definition/cybersecurity

23. Sico van der meer&franspaul van der putten , US deterrence against chinese cyber espoinage**, policy brief** , clingendael , netherlands institute of international relations , september 2015 . link seen in 15/02/2019 :
https://www.clingendael.org/sites/default/files/pdfs/