HNSJ Humanitarian & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net
مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير العربي للعام 2020 = 0.44

عنوان البحث

فرص دولة قطر في التعاون السيبراني مع حلف شمال الأطلسي (الناتو)

عبد الرحمن سعيد الكواري[1]

[1] باحث في مجال الدراسات الأمنية النقدية

بريد الكتروني: aal061@dohainstitute.edu.qa

HNSJ, 2021, 2(11); https://doi.org/10.53796/hnsj21112

تاريخ النشر: 2021/11/01م تاريخ القبول: 2021/10/12م

المستخلص

تحت ظل التطور المستمر للتكنلوجيا توجد تهديدات عديدة يمكن للقراصنة الالكترونيين والمخربين من استغلالها لتحقيق مأرب غير سرعية. بينما تسعى الدول للاعتماد على أحدث البرامج لحماية أنفسها، نشأت تحت قيادة حلف شمال الأطلسي تحالفاً وتعاوناً لصد الهجمات الإلكترونية وبناء سياسات تساعد الدول الأعضاء من تطوير دفاعاتها السيبرانية. تهتم هذه الورقة بدراسة الفرص التي يمكن لقطر استغلالها لتعزيز قدراتها السيبرانية بعد تعاونها مع حلف شمال الأطلسي. وتستخدم الورقة منهجية دراسة الحالة لفهم وتحقيق ذلك.

RESEARCH ARTICLE

QATAR'S OPPORTUNITIES IN CYBER COOPERATION WITH THE (NORTH ATLANTIC TREATY ORGANIZATION (NATO))

Abdul Rahman Saeed Al-Kuwari[1]

[1] researcher in critical security studies

HNSJ, 2021, 2(11); https://doi.org/10.53796/hnsj21112

Published at 01/11/2021 **Accepted at 12/10/2021**

Abstract

Under the continuous development of technology, there are many threats that hackers and saboteurs can exploit to achieve a non-speedy purpose. As countries seek to rely on the latest programs to protect themselves, under the leadership of NATO, an alliance and cooperation has emerged to fend off cyberattacks and build policies to help member states develop their own cyber defenses. This paper studies the opportunities that Qatar can exploit to enhance its cyber capabilities after its cooperation with NATO. The paper uses case study methodology to understand and achieve this.

المقدمة

تعاني الدول من هجمات واختراقات سيبرانية، وقد تتعرض بعض الدول الضعيفة في مجال الأمن السيبراني إلى هجمات منظمة من قبل دولة أخرى، يوضح سيناريو اختراق وكالة الانباء القطرية ذلك، تسعى غالباً الدول لبناء سياسات تعزز فيها من قدراتها وامكانياتها في مواجهة التحديات المختلفة. يكون ذلك عن طريق التحالفات مما يشكل لها شبكة متينة من العلاقات التي تتيح لها أمكانيات وتقنيات متنوعة يمكن الاستفادة منها ضد أي تهديد يحول في الأفق. تهتم الورقة بدرس النموذج القطري وإمكانية الاستثمار في تحالفه مع حلف شمال الأطلسي لتطوير قدراته السيبرانية. حيث يوجه البحث اهتمامه على ثلاث جوانب مهمة:

الأولى: المشكلة التي تعانيها قطر في تأمينها لمجالاتها السيبرانية، وسيتم استخلاص نقاط الضعف عن طريق دراسة اختراق وكالة الانباء القطرية "قنا".

الثانية: الجهود الدبلوماسية التي تتيح لقطر التعاون مع الناتو في المجالات السيبرانية، وبناً على دراسة مستوى التعاون والمميزات التي يمكن لقطر الاستفادة منها، ستأتي في المرحلة الثالثة.

الثالثة: الإمكانيات التي بحوزة الناتو، وفرص قطر في الاستفادة منها.

تكمن أهمية هذه الورقة في تعزيز رؤية قطر لمواكبة التطور التقني المستمر والسريع في مجال الامن السيبراني، وسيكون ذلك عن طريق الإجابة على السؤال البحث: كيف يمكن لدولة قطر الاستفادة من تحالفها مع الناتو لتعزيز استراتيجية الدفاع السيبراني لديها؟ كما سيعتمد البحث على منهج دراسة الحالة في سبيل تحقيق ذلك.

حيثيات اختراق وكالة الانباء القطرية (قنا)

بالرغم من قيام قطر باعتماد استراتيجية أمن سيبراني في 2014 مرتكزة على تحقيق مستوىً عالٍ من الحماية تحمي بها المنشآت الحيوية وتسطيع من خلالها التصدي للهجمات السيبرانية في الوقت المناسب[1]، إلا أن ذلك لم يكن كافياً، إذ تمكنت مجموعة من القراصنة باختراق وكالة الأنباء القطرية في تاريخ 23 مايو 2017. استخدم المخترقون تقنيات مبتكرة من خلال استغلال ثغرة إلكترونية على الموقع الإلكتروني للوكالة[2]، وتوضح وزارة الداخلية القطرية أن المخترقين قاموا بعملية استطلاع الكترونية لموقع الوكالة لتحديد نقاط الضعف وتمت العملية في تاريخ 19 أبريل 2017[3]باستخدام برمجيات متعددة[4]. يفسر مختصون في المجال أن المخترقين قاموا باستخدام تكتيك الاصطياد بالرمح "Spear Phishing[5]" لاختراق أحد هواتف الموظفين في الوكالة واستخدامه

---

[1] QATAR NATIONAL CYBER SECURITY STRATEGY, Qatar government, PP vi– vii, 2014, https://bit.ly/32kxjEW

[2] تصريح لوزارة الداخلية بشأن قرصنة موقع وكالة الأنباء القطري، وزارة الخارجية، https://bit.ly/3iXqC1U

[3] المؤتمر الصحفي لوزارة الداخلية القطري حول قرصنة وكالة الأنباء القطرية، التلفزيون العربي، الدقيقة 4:00 الى 4:30 الى 2:00، 2017، https://bit.ly/2RZBFf2

[4] بحسب المؤتمر الصحفي الذي تناوله فيه وزارة الداخلية القطرية كيفية الاختراق، فقد ذكرت الوزارة ان البرمجيات المستخدمة هي: ((PureVPN, Offshore Dedicated Privacy Made Easy, Private internetaccess)) .

[5] According to Mohammed Aldorani, this is similar to fishing, the term used to phis for any vulnerable target in collecting user's credentials such as user identification and passwords, and any other related security

كنقطة عبور لجهاز الخادم الرئيسي وبذلك كانت وسائل الاتصال عن بعد بين أجهزة الموظفين الشخصية والجهاز الرئيسي للوكالة أحد الثغرات التي تسمح بوصول الفيروسات للجهاز[6]، وفي تحقيقات لاحقة أُعلنت على وسائل الاعلام القطرية تبين أن المخترقين استخدموا شركة وهمية في أذربيجان للتعامل مع مختصين في المسح والكشف عن الثغرات لأمنية في شبكة الوكالة، حيث أنهم قدموا إليهم مجموعة من المواقع لتفحصها بحجة أن الشركة تقوم بإصلاحها، وكان من ضمن تلك المواقع موقع وكالة الانباء القطرية[7]. تمكن المخترقون من السيطرة على حسابات الوكالة في منصات وسائل التواصل الاجتماعي[8]. بحسب التقارير المعلنة من وزارة الداخلية القطرية أن تحميل البرمجيات الخبيثة تمت في 22 إبريل 2017 في تمام الساعة 3:40 صباحاً، ومن ثم قام المخترقون بإجراء بعض التعديلات على البرمجيات الخبيثة التي تم تحميلها من قبلهم في الجهاز الرئيسي ليمكنهم من التحكم الكامل في الشبكة مما سمح لهم بالحصول على كافة العناوين والأرقام السرية للشبكة. تؤكد التقارير ان المخترقين قاموا بالدخول للشبكة عدة مرات للتأكد من قدرتهم على الهجوم[9]. ويستنتج من ذلك:

1- اتصال الموظفين مع الخادم الرئيسي للوكالة عن طريق هواتفهم أو أجهزة متصلة بالإنترنت، غير مؤمنه ضد الهجمات، مما تجعلها نقطة عبور للخادم الرئيسي.

2- ضعف في قدرة النظام على الكشف عن الفيروسات، حيث أنهُ تم تحميل برمجيات خبيثة ساعدت على التحكم بالشبكة ولم يتمكن النظام من كشفها.

تحالف قطر مع الناتو

تهتم قطر بتعزيز قدراتها السيبرانية بمختلف الطرق، ويعتبر التحالف مع الناتو خطوة أساسية في هذا الاتجاه، ويوضح وزير الخارجية القطري ذلك " نحن في قطر نركز تعاوننا في مجالات العمل المشترك والتدريب والتعليم والدفاع السيبراني وأمن الطاقة والتخطيط لمواجهة الطوارئ المدنية وإدارة الأزمات"[10]. سيساعد ذلك قطر في تطوير قدراتها عن طريق الاستفادة من تقدم الدول الأعضاء في حلف الناتو في مجال الأمن السيبراني. تُؤكد الخارجية القطرية رغبة قطر في تحقيق الأمن السيبراني ومواجهة التحديات السيبرانية من خلال التعاون مع حلف الناتو[11]. يساعد التحالف المشترك بين قطر والناتو على انخراطها في سياسات الردع والدفاع وتعزيز الأمن بين أطراف الحلف، حيث قامت قطر بالمشاركة في القمة رقم 29 لحلف الناتو، والتي تضمنت جلسات لتطوير هيكل

---

passwords. Spear Phishing is more a targeted approach to attack whereby a hacker would look for a specific target to attack. Both terms are most popular as this hacking method has become widespread.

[6]محمد الدوراني، تأثير الهجمات السيبرانية على البنى التحتية.. الحرب السيبرانية ودول مجلس التعاون الخليجي، معهد الدوحة للدراسات العليا، قطر، تم البث عن طريق الحساب الرسمي للمعهد في توتر، 2020، الدقيقة 33 الى 34، https://bit.ly/2ZX2bds

[7]عام على اختراق "قنا".. هكذا قرصنت دول الحصار عقول شعوبها، الخليج أونلاين، 2018، https://bit.ly/30r70MD

[8]المؤتمر الصحفي لوزارة الداخلية القطري حول قرصنة وكالة الأنباء القطرية، الدقيقة 1:40 الى 2:00.

[9]المؤتمر الصحفي لوزارة الداخلية القطري حول قرصنة وكالة الأنباء القطرية، الدقيقة 4:40 الى 5:00.

[10]نائب مجلس الوزراء وزير الخارجية يجتمع مع الأمين العام لحلف شمال الأطلسي الناتو، وزارة الخارجية القطرية، 2019، https://bit.ly/38FTvh0

[11]المصدر السابق.

حلف الناتو ليتلاءم مع متطلبات الاستجابة السريعة للأزمات، ودور قطر والدول الأخرى في الاستجابة لها[12]. ويوضح وزير الخارجية التركي مولود تشاوش أوغلو أن التحالف القطري مع الناتو سيتضمن تحالفاً على المستوى العسكري وتعاوناً على الصعيد المادي لتحقيق رادع فعال ضد التهديدات الأمنية[13]، كما يعزز التحالف من مرونة المبيعات في المجال العسكري بين قطر والدول الأعضاء في الناتو، يوضح مساعد وزير الخارجية الأميركي لشؤون الخليج العربي تيموثي لاندركينغ أن التحالف "سيسمح لقطر بالاستفادة من مزايا في مجال التجارة العسكرية والتنسيق الأمني"[14]. ايضاً يجب الإشارة الى التسهيلات في المبيعات التي يكمن لقطر الحصول عليها، والتي ستساعد في تطوير الدفاعات القطرية في عدة جوانب منها الجانب السيبراني، فبحسب إبراهيم السعيدي الخبير في شؤون حلف شمال الأطلسي "تكمن في تكثيف التعاون مع قطر في الجوانب العسكرية والدفاعية من خلال تسهيل إجراءات شراء الأسلحة والتكنولوجيا العسكرية المتقدمة والأنظمة الأمنية المتطورة، علاوة على استفادة قيادات الدفاع من الدورات التكوينية المشتركة مع الجيش الامريكي"[15]، وتسعى قطر لتطوير هذه العلاقات بشكل مستمر لتستطيع تحقيق ردع فعال من اعتداءات خصومها، لذلك تقوم بتكثيف المحادثات وتطوير العلاقات مع الناتو، يصف جلال سلمي أحد المتخصصين في العلاقات الدولية، أن هذه العلاقات " تُعلي من رصيد قطر الإقليمي كدولة صغيرة المساحة كبيرة النفوذ"[16].

بحسب ما سبق ذكره يمكن استخلاص أن هنالك ثلاث فرص رئيسية ستمكن قطر من الاستفادة من الناتو لتعزيز قدراتها السيبرانية:

الاول: تسهيل للمبيعات العسكرية ومنها البرمجيات وأنظمة الدفاع السيبراني.

ثانياً: التدريب في المجالات المختلفة والتي تشمل الجانب السيبراني.

ثالثاً: التنسيق الأمني الذي قد يدعم قطر في مجالات عدة مثل تبادل المعلومات.

القدرات السيبرانية للناتو

تلعب الشراكات القوية بين الدول الأعضاء في الناتو دورًا رئيسيًا في معالجة التحديات السيبرانية بفعالية، ركز الناتو على وضع التدابير لتلبية المتطلبات الأمنية، حيث حددت قمة مجلس شمال الأطلسي للناتو (NAC) لعام 2002، التي أُقيمة في جمهورية التشيك، دخول الدفاع الإلكتروني كقضية مهمة تستحق الاهتمام الجماعي للحلف[17]، ويوضح الجنرال فولفجانج رينر نائب رئيس أركان الفضاء السيبراني للناتو أن تحديات الفضاء السيبراني

[12] مسؤولة في الناتو: انضمام قطر إلى الحلف مهم جداً، صحيفة الشرق، 2018، https://bit.ly/3ltvIEj

[13] مريم بومديان، وزير خارجية تركيا لـ الشرق: قطر طرف وازن في معادلة القوى الدولية لمواجهة الإرهاب، صحيفة الشرق، 2018، https://bit.ly/3eWX5o4

[14] واشنطن: نعمل لإعلان قطر حليفاً رئيسياً من خارج الناتو.. وهذه المزايا التي ستحصل عليها، صحيفة الشرق، 2020، https://bit.ly/3ktOvOs

[15] الوالي أحمد، خبير بشؤون "الأطلسي": هذه دلالات إعلان قطر حليفاً رئيساً للناتو، الخليج أونلاين، 2020، https://bit.ly/2GdJs6L

[16] أحمد يوسف، قطر.. حليف رئيسي للناتو يسعى لعضوية كاملة، الانظول وكالة الانباء التركية، 2020، https://bit.ly/3eWssil

[17] Jeffrey L.Caton, NATO cyberspace capability: a strategic and operation evolution, U.S. Army College, P2,2016, https://bit.ly/32rIGv0

تؤثر على الدفاعات السيبرانية للناتو، ويجب أن يتسم موقفنا التشغيلي بالمرونة والتكيف والتعاون[18]. أدت الهجمات السيبرانية على إستونيا في 2007 والتي اتبعت تكتيكات مثل "تكتيك رفض الخدمة– DDOS"[19]، حيث كانت إستونيا تعتمد بشكل كامل في معاملاتها الحكومية والمصرفية على الانترنت، وتسببت الهجمات التي جاءت على شكل موجات على مدار ثلاثة أسابيع بتعطيل قدرة المستخدم من الانتفاع بالخدمات[20]. يوضح جيمس لويس من مركز الدراسات الاستراتيجية والدولية أن هجمات DDoS "تستخدم بشكل أكثر شيوعًا في الأنشطة غير المشروعة[21]، حيثُ وجَّه المهاجمون ما يقرب من مليون جهاز كمبيوتر في استونيا للتقدم بعدد هائل من الطلبات في نفس الوقت، مما أدى إلى زيادة حركة المرور إلى ما هو أبعد من المستويات العادية من النشاط وبالتالي إيقاف الخوادم[22]. توالت الهجمات على دول أعضاء بالناتو، ففي 2008 وقعت هجمات إلكترونية على جورجيا مشابهه لسابقتها، فقد استهدفت الهجمات على مواقع حكومية منها موقع مكتب رئيس جورجيا كما قام المخربين بختراق قناتان تلفزيونية[23]، وتبع المخربون تكتيك رفض الخدمة (DDoS) وأشارت إلى أن هجمات DDoS تزامنت مع تحرك القوات الروسية إلى أوسيتا الجنوبية ردًا على العمليات العسكرية الجورجية. تسببت هجمات DDoS في تعطيل معظم مواقع الويب الحكومية الجورجية[24]، دفع ذلك الناتو لإعادة النظر في استراتيجيته الأمنية السيبرانية[25]، ووضع أول سياسة دفاع إلكتروني في 2008، وفي عام 2014 جعل الناتو الدفاع الإلكتروني جزءًا أساسيًا من الدفاع الجماعي معلناً أن هجومًا إلكترونيًا يمكن أن يؤدي إلى تطبيق بند الدفاع الجماعي (المادة 5) من المعاهدة التأسيسية لحلف الناتو علاوة على ذلك، في عام 2016 اعترف الحلفاء بالفضاء الإلكتروني كمجال للعمليات العسكرية، وتعهدوا كذلك بتعزيز الدفاعات السيبرانية لشبكاتهم وبنيتهم التحتية الوطنية كمسألة ذات أولوية[26]. أما على الصعيد الفني فقد قام الناتو بتطوير قدراته للكشف والتصدي للهجمات الالكترونية، وعلى صعيد الموارد البشرية فقد قام بتوظيف قدراته في التخطيط لوضع استراتيجيات وسياسات تحقيق الأمن السيبراني، ويخصص الناتو مبالغ كبيرة لتطوير برمجيات الجدار الناري لديهم، كما ساهم

---

[18] NATO LEADERS CALL FOR GREATER COLLABORATION IN CYBERSPACE, Vigilia Pretium libertatis, NATO, https://bit.ly/3kc7LA1

[19] Emilio Iasiello, Cyber Attack: A Dull Tool to Shape Foreign Policy, International Conference on Cyber Conflict, P2, 2013, https://bit.ly/3exmd4u

[20] مايا أوتاراشفيلي، القرصنة الروسية ليست جديدة...الحرب الالكترونية الأولى في أستونيا، المجلة، 2017، https://bit.ly/3f2ymOX

[21] STEPHEN W. KORNS and JOSHUA E. KASTENBERG, Georgia's Cyber Left Hook, ARMY WAR COLLEGE CARLISLE BARRACKS PA STRATEGIC STUDIES INSTITUTE, P60, 2009, https://bit.ly/3n4eWvM

[22] Vincent Joubert, Five years after Estonia's cyber attacks: lessons learned for NATO, Research Division, NATO Defense college, Rome, NO. 76, P1, 2012, https://www.files.ethz.ch/isn/143191/rp_76.pdf

[23] بريطانيا وأميركا تساند جورجيا بتحميل روسيا مسؤولية استهدافها بهجمات إلكترونية، شبكة الجزيرة الإعلامية، 2020، https://bit.ly/38FpwFF

[24] المصدر السابق، ص 64.

[25] التهديدات الجديدة: الأبعاد الالكترونية، مجلة الناتو، حلف شمال الأطلسي (الناتو)، https://bit.ly/3kRTLfN

[26] Laura Brent, NATO'S role in cyberspace, NATO, 2019, https://bit.ly/2U16Qrk

التقدم التكنولوجي لدى الدول الأعضاء في الحلف إلى تطوير الصناعات التقنية مثل خط إنتاج جهاز FAST360 الخاصة بشركة Arkoon حيثُ تَدمج أجهزة FAST360 مجموعة كاملة من تقنيات الأمان (جدار الحماية، VPN، مكافحة الفيروسات، مكافحة البريد العشوائي) كما يقدم خدمات الشبكة مثل (NAT، VLAN ، التوجيه الديناميكي) وميزات QoS (إدارة النطاق الترددي)[27]. ساهمت القوائم المشتركة بين دول الأعضاء في الناتو من تعزيز قدرات الجدار الناري للناتو، حيثُ قاموا بإنشاء قائمة يطلق عليها اسم "قائمة بصمة الفيروسات" والتي يتم تحديثها بشكل مستمر لتمكن برمجيات مكافحة الفيروسات (الجدار الناري) من كشف الفيروسات الخبيثة. يقوم مركز الاتصال والمعلومات في للناتو بإدارة عدة وكالات فرعية وتقدم أكثر من 150 خدمة في مجالات متعددة منها (التدريب، التخطيط، تقديم المعلومات، تقديم الدعم التقني في مجالات مختلفة، وغيرها...)[28]، من ضمن هذه الوكالات مركز الأمن السيبراني الذي يقدم مميزات مهمة قد تستفيد منها قطر، مثل المشاركة في تبادل المعلومات والثغرات الأمنية بين دول الاعضاء والدول المشاركة[29]، ويقدم المركز مشروع الدفاع السيبراني متعدد الجنسيات والذي يقوم بتطوير عدة جوانب من الأمن السيبراني من خلال تشارُك عدة دول لتطوير البرمجيات الأمنية، حيث يغطي مواضيع مثل (تطوير برمجيات الإنذار السيبراني المبكر، تطوير وسائل الكشف عن التهديدات ورصدها، تطوير برمجيات تخفيف الهجمات الإلكترونية من خلال الاستجابات شبه الآلية' وغيرها ...)[30]. يتضمن هيكل الدفاع السيبراني في الناتو مركز الناتو للاستجابة للهجمات الالكترونية (NCIRC) [31]، المكون من 200 خبير وهذه الهيئة مختصة بحماية شبكة الناتو والحفاظ على معلوماتها من القرصنة وتصنف كهيئة دفاعية [32]. طور الناتو تقنيات تساعده في الحروب التقليدية ويشرف مركز عمليات الفضاء الإلكتروني (CYOC) على دعم القدرات التقليدية والنووية بقدرات هجومية إلكترونية يمكنها أن تعزز تقدم الجيش على الارض[33]. تسمح الإجراءات الموضحة من قبل للناتو فيما يتعلق بالاستجابة السريعة والفعالة في حالة حدوث أزمة إلكترونية، حيث يوفر فريق التدخل السريع استجابة فنية منسقة. كما يتيح تبادل المعلومات بين وكالات الناتو فرصة أكبر لكشف هوية المعتدي[34]، وغالباً ما تكون فرق التدخل السريع التابعة للناتو فرق صغيرة مكونه

---

[27] Arkoon FAST360 A10, NATO, https://bit.ly/36volGr

[28] What we do, NATO Communications and Information Agency (NCIA), https://bit.ly/3l4ZP4W

[29] NATO's Cyber Security Centre, NATO Communications and Information Agency (NCIA), https://bit.ly/2l0upOV

[30] Multinational Cyber Defence Capability Development (MN CD2), NATO Communications and Information Agency (NCIA), https://bit.ly/3exvYzv

[31] قطر.. مجلس الوزراء يوافق على إنشاء وكالة للأمن السيبراني، الخليج أونلاين، 2020، https://bit.ly/32ga0fy

[32] NATO Cyber Defence, NATO, 2019, https://bit.ly/3mPRwu0

[33] LILLIAN ABLON, ANIKA BINNENDIJK, QUENTIN E. HODGSON, BILYANA LILLY, SASHA ROMANOSKY, DAVID SENTY, JULIA A. THOMPSON, Operationalizing Cyberspace as a Military Domain, RAND corporation, P 8, 2019, https://bit.ly/3kW4yFU

[34] Vincent Joubert, Five years after Estonia's cyber attacks: lessons learned for NATO, Research Division, P 4.

من 4 إلى 6 أشخاص[35]. توفر رابطة الدول المستقلة التابعة لحلف الناتو في بلجيكا خبراء في تكنولوجيا المعلومات قابلين للانتشار في دول الحلفاء للدعم التشغيلي والتقني[36]. بالإضافة الى ذلك، يلقي الناتو اهتماما كبيراً في تطوير الموارد البشرية من خلال التركيز على توظيف الخبرات في مجال الأمن السيبراني. ويهتم بنشر الثقافة الأمنية الفضاء الالكتروني بين الموظفين غير المتخصصين في مجال الأمن السيبراني، من خلال إنفاق ميزانيات طائلة من أجل نشر الوعي الأمني للفضاء السيبراني لدى العاملين في المؤسسات والمواقع الحساسة في دول الاعضاء[37]. كما يقوم مركز الاتصال والمعلومات في للناتو بإدارة تقديم الدعم الاستشاري من خلال الخبراء، تقديم الدورات التدريبية في مجال الأمن السيبراني[38]. لضمان التنسيق المستمر والتطوير للاستراتيجيات المتبعة للأمن السيبراني يقيم الناتو تدريبات سيبرانية سنوية تهدف الى الاستجابة للسناريوهات المختلفة والتي يمكن وقوعها كما تهدف للتكامل في التنسيق بين دول الأعضاء على جميع المستويات التكتيكية والاستراتيجية[39]، ويمثل تمرين لوك شيلد "Locked Shields" أحد الأمثلة التي تُمكّن هذه التمارين الخبراء في مجال الأمن السيبراني من تعزيز مهاراتهم في الدفاع عن أنظمة تكنولوجيا المعلومات الوطنية والبنية التحتية الحيوية في ظل هجمات الوقت الفعلي. ينصب التركيز على السيناريوهات الواقعية والتقنيات المتطورة ومحاكاة التعقيد الكامل للحادث السيبراني الضخم، بما في ذلك اتخاذ القرارات الاستراتيجية والجوانب القانونية والاتصالات[40]، إنه تدريب الفريق الأحمر مقابل الفريق الأزرق، حيث يتم تشكيل الأخير من قبل الدول الأعضاء في مركز التميز التعاوني للدفاع السيبراني التابع لحلف الناتو(CCDCOE[41])، تلعب الفرق الزرقاء المشاركة دور فرق الرد السريع الوطنية التي يتم نشرها لمساعدة دولة خيالية في التعامل مع الحوادث السيبرانية واسعة النطاق وجميع تداعياتها المتعددة. بالإضافة إلى الحفاظ على حوالي 4000 نظام افتراضي أثناء مواجهة أكثر من 2500 هجوم، يجب أن تكون الفرق فعالة في الإبلاغ عن الحوادث وتنفيذ القرارات الاستراتيجية وحل تحديات الطب الشرعي والقانونية والإعلامية. لمواكبة التطورات التكنولوجية، تركز لوك شيلد على سيناريوهات واقعية وتقنيات متطورة وشبكات ذات صلة وطرق هجوم[42]، ولقد استفادة دول عدة حليفة للناتو مثل الأردن من المشاركة في التمارين لتعزيز قدراتها

---

[35] Z'hra M. Ghavam, NATO'S PREPAREDNESS FOR CYBERWAR, NAVAL POSTGRADUATE SCHOOL, p 44, 2016, https://bit.ly/32ocfxu

[36] المصدر السابق.

[37] Neil robinson, Spending for success on cyber defence, NATO Review, 2017, https://bit.ly/3jYW4fX

[38] What we do, NATO Communications and Information Agency (NCIA), https://bit.ly/3l4ZP4W

[39] LILLIAN ABLON, ANIKA BINNENDIJK, QUENTIN E. HODGSON, BILYANA LILLY, SASHA ROMANOSKY, DAVID SENTY, JULIA A. THOMPSON, Operationalizing Cyberspace as a Military Domain, P 12.

[40] Locked Shields, CCDCOE, The NATO Cooperative Cyber Defence Centre of Excellence, https://bit.ly/3p1RBgp

[41] وهوَ مركز مختص بتطوير وتعزيز القدرات السيبرانية لدى الناتو، كما يهتم بتطوير العقيدة والمفهوم ، والوعي والتدريب، والبحث والتطوير، والتحليل والدروس المستفادة.

[42] المصدر السابق

الأمنية وسد الثغرات السيبرانية[43]. يقيم الناتو عدة تمارين تعبويه للجيش في المجال السيبراني مثل تمرين سيبر كوليشون وشارك فيه 28 دولة، يوضح مدير التمرين المقدم أندريس كوسك طبيعة التمرين "توم الفرق الفنية بتحديد وتحلل وتوقف البرامج الضارة شديدة التعقيد"[44]. أصدر الناتو دليل تلين ميل 2.0 في سبيل تحليل سلسلة التشريعات القانونية في عالم الفضاء السيبراني وتصنيف الهجمات التي قد ترقى لحرب سيبرانية[45]، يهدف الدليل الذي يتم تطويره من فترة إلى أخرى إلى وضع تحليل منطقي يربط المبادئ الرئيسية التي يجب أن تُخذ في الحسبان عند الحروب بالعالم السيبراني، مثل التشريعات القانونية وحقوق الانسان.

فرص قطر في الاستفادة من الناتو

تعمل العديد من الدول الأعضاء في الناتو بمجال تطوير البرمجيات الدفاعية لتأمين منشئاتها كما تمتلك بعض الدول مثل الولايات المتحدة وبريطانيا قدرات سيبرانية هجومية وأخرى في التجسس الإلكتروني[46]، يعمل حلف شمال الاطلسي تحت نظام حماية مركزي ضد الهجمات عبر الفضاء الالكتروني[47]، وفي ظل جميع المعطيات السابقة يمكن الاستفادة من ذلك في تعزيز أمنها السيبراني عبر المجالات التالية:

أولاً: الإصلاحات الداخلية

هنالك عدة إجراءات يمكن لقطر اتخاذها قبل النظر في فرص التحالف مع الناتو، وتعتبر هذه الاجرائات إجراءات احترازية من أجل المحافظة على الأمن السيبراني. يمكن ان يشكل منع اتصال الموظفين عبر أجهزتهم الشخصية بالخادم الرئيسي للوزارة أو المؤسسة أو حتى الشركات المساهمة اجراً يمنع من استخدام الأجهزة الشخصية كنقطة عبور. كما يفسر العديد من المختصين بعض النواحي التي يجب إعادة النظر فيها لكي تتمكن قطر من تحقيق أمنها السيبراني، يوضح محمد الدوراني أحد المتخصصين في مجال الأمن السيبراني ومدير سابق للحاسب الالي في الأمانة العامة بمجلس التعاون، أن هنالك عدة ركائز يجب على قطر أن تتبناها إذا ما أرادة أحراز تقدم فعال في هذا المجال منها:

1- إنشاء مركز للسيطرة والتحكم السيبراني بغرض الدفاع عن البنية التحتية الالكترونية، ويجب أن يتمتع هذا المركز بصلاحيات مباشرة الكيانات الحاسوبية في المؤسسات المختلفة.

---

[43] CYBER COALITION 16: NATOS LARGEST CYBER DEFENCE EXERCISE, Vigilia Pretium libertatis, NATO, https://bit.ly/3pa1rgc

[44] NATO EXERCISE CYBER COALITION 17 UNDERWAY IN ESTONIA, Vigilia Pretium libertatis, NATO, https://bit.ly/32peKPW

[45] Tallinn Manual 2.0, CCDCOE, The NATO Cooperative Cyber Defence Centre of Excellence, https://bit.ly/36bRw0R

[46] JAMES A. LEWIS, THE ROLE OF OFFENSIVE CYBER OPERATIONS IN NATO'S COLLECTIVE DEFENCE, The Tallinn Papers, NO.8, P7, 2015, ***https://bit.ly/3n89rwp***

[47] انخراط نشاط ونظام دفاعي حديث، تبناه قادة والحكومات في لشبونة "المفهوم الاستراتيجي للدفاع والأمن للدول الأعضاء في منظمة حلف شمال الأطلسي"، حلف شمال الأطلسي (الناتو)، 2010، https://bit.ly/3mJWUij

2- عدم التعامل عن بُعد مع الحاسوب الرئيسي المتصل بالبنية التحتية الالكترونية، ويقصد بعدم التعامل عن بعد أي عدم استخدام الهاتف أو الأجهزة الذكية الأخرى لتوقيع البريد لدى المسؤولين أو اعتماد المعاملات عن بعد.

3- الاعتماد على الكوادر الوطنية لتأمين البنية التحتية السيبرانية، وذلك أن في حال الاعتماد على بعض الشركات الأجنبية قد يتسبب في تسريب معلومات عن نظام الحماية المتبع لدى هذه المؤسسات[48].

يوافق على ذلك أحمد محمد بني عيسى أحد الخبراء المختصين في إدارة الأزمات الالكترونية، ان من المهم الاستثمار في الموارد البشرية المحلية وتقليل الاعتماد على الشركات الأجنبية في وظيفة تأمين الشبكات والبنية التحتية السيبرانية. يمكن ذلك من خلال تخصيص ميزانيات تساعد الموارد البشرية على الحصول على البرمجيات اللازمة في تأمين الفضاء السيبراني الخاص بقطر[49]. نظراً لتوجه قطر نحو استخدام الانترنت في تعاملاتها اليومية، حيث أصبحت هنالك العديد من المواقع الحكومية التي تقدم الخدمات للمستفيدين، توصي الدراسة بوضع حد معين لاستقبال الطلبات، وذلك عن طريق وضع رقم معين إذا وصلت الطلبات لهذا الرقم يقوم الجهاز بتعليق الطلبات مؤقتاً حتا تتم الانتهاء من جزء من الطلبات السابقة، وبذلك يستطيع استقبال الطلبات المعلقة على شكل دفعات والتي تتيح ضبط الحركة المرورية لتدفق الطلبات خلال الموقع.

الإصلاحات من خلال خبرات الناتو

فرص تطوير البرامج وسد الثغرات التقنية

1- تمكن مخربو قناة قنا من التسلل ووضع برمجيات خبيثة دون تمكن برمجيات الحماية من كشفهم، لذلك هنالك فرصة من الاستفادة من الجدار الناري الذي يطوره الناتو، كجزء من جدار ناري وطني يحمي جميع الشبكات القطرية.

2- يمكن لقطر أن تسد ثغرات أمنية في شبكاتها إذا ما تمكنت من الحصول على قائمة بصمة الفيروسات تحت بند تبادل المعلومات المبرمة مع الناتو في اتفاقية التعاون.

3- يمكن كذلك من خلال التسهيلات المقدمة أن تحصل على عقود مبيعات لأنظمة أمن سيبرانية متطوره

4- يلزم قطر تقديم الدعم المالي للناتو كجزء من الاتفاقية، لذلك يمكن أن تستثمر قطر أموالها في مشاريع تعود عليها بفائدة أكبر من غيرها مثل الاستثمار في مشروع الدفاع السيبراني، الذي يقوم على تطوير برمجيات الكشف على النظام، وبرمجيات الإنذار المبكر، وغيرها من البرمجيات.

فرص تطوير الموارد البشرية

1- يمكن التعاون مع مركز الأمن السيبراني التابع للناتو لتقديم دورات تدريبية للكوادر القطرية.

2- يمكن الاستفادة من خطة الناتو لنشر الوعي الأمني في المجال السيبراني لغير العاملين في المجال، لتثقيف الموظفين في الوزارات والهيئات الحكومية والقطاع الخاص في قطر.

فرص تطوير الجيش القطري

[48] محمد الدوراني، قتال غير مرئي: الحرب السيبرانية في الأزمة الخليجية، مركز الجزيرة للدراسات، ترجمة: كريم الماجري، ص 9، 2018.

[49] أحمد محمد بني عيسى، دور إدارة الازمات الالكترونية في حماية المنشئات الحيوية، دراسات أمنية استراتيجية، وزارة الداخلية القطرية، العدد الاول، ص 18، 2020.

1- يمكن الاستفادة من التقنيات التي يقدمها مركز عمليات الفضاء الالكتروني، لدعم القوات المسلحة القطرية بتقنيات تساعدها في المناورة ضد الأعداء.

2- يمكن الاستفادة من التدريبات التي يقيمها الناتو في تطوير الخبرات وتنسيق الجهود في حالة الهجمات السيبرانية المنظمة.

فرص تعزيز قدرات القيادة والسيطرة القطرية

بعد انشاء وكالة الأمن السيبراني في قطر، يمكن للقائمين على الوكالة الاستفادة من خبراء واستشاريي الاتصالات والمعلومات لدى الناتو في وضع أسس القيادة والسيطرة السيبرانية، كما يمكن الاستفادة من فرق التدخل السريع للناتو في تقديم الدعم الفني في حالة الازمات.

الخاتمة

استند البحث على ثلاث ركائز أساسية، الاولى وهي معرفة الثغرات عن طريق دراسة اختراق وكالة قنا، ثم معرفة ما يمكن أن تقدمة الاتفاقية مع حلف الناتو لقطر، ومن ثم تحديد القدرات التي يمتلكها الناتو في المجال السيبراني وكيفية الاستفادة منها. في النهاية وبناءً على الحاجة القطرية وما يمكن الحصول عليه تم تقديم عدة توصيات، استهدف البحث قطر لتصبح مثالاً يحتذى به كدولة صغيرة ذات علاقات متينة حيث يمكن الاستفادة من هذا النموذج في التخطيط للاستفادة من العلاقات والتحالفات لتوفير الأمن في شتى المجالات وخصوصاً السيبراني منها. كما قدم البحث عدة توصيات على المستوى التنفيذي والتكتيكي الذي يمكن لقطر من خلاله أن تعزز قدراتها السيبرانية وفي فترة بسيطة حيث بدئت التوصيات بإصلاحات داخلية وهي أساسية وبتوصية خبراء في المجال، ثم امتدت إلى سبل الاستفادة من التعاون بينها وبين الناتو، ويمكن لقطر أن تحقق ذلك بسهوله إذ أن الموارد البشرية والمادية متوافرة لديها وتوجد هنالك فرصة لتسريع عجلة التنمية وتطوير البنية التحتية إذا ما استغلت قطر تحالفها مع الناتو الذي أثبت أنه في خلال سنوات قليلة أصبح قوة سيبرانية فعالة.

المصادر والمراجع

المصادر العربية

محمود، قاصد، جواد الحمد، عاطف الجولان، عبد الحميد فخري، "الأزمة الخليجية 2017 البُعد الآخر، 2017، http://bit.ly/2OseJ7J

مرور عام على اختراق وكالة الأنباء القطرية (قنا)، مكتب الاتصال الحكومي، 2018، https://bit.ly/2JGiupK

تصريح لوزارة الداخلية بشأن قرصنة موقع وكالة الأنباء القطري، وزارة الخارجية، https://bit.ly/3iXqC1U

المؤتمر الصحفي لوزارة الداخلية القطري حول قرصنة وكالة الأنباء القطرية، التلفزيون العربي، الدقيقة 4:00 الى 4:30 الى 2:00، 2017، https://bit.ly/2RZBFf2

محمد الدوراني، تأثير الهجمات السيبرانية على البنى التحتية.. الحرب السيبرانية ودول مجلس التعاون الخليجي، معهد الدوحة للدراسات العليا، قطر، تم البث عن طريق الحساب الرسمي للمعهد في توتر، 2020، الدقيقة 33 الى 34، https://bit.ly/2ZX2bds

عام على اختراق "قنا".. هكذا قرصنت دول الحصار عقول شعوبها، الخليج أونلاين، 2018، https://bit.ly/30r70MD

ما خفي أعظم – ليلة القرصنة، قناة الجزيرة، 2018، الدقيقة 4:00 الى 4:30، https://bit.ly/2GeMgjW

الاستراتيجية الوطنية للأمن السيبراني، وزارة المواصلات والاتصالات، https://bit.ly/38mnDOe

تحقيق للجزيرة: قرصنة "قنا" تمت من وزارة سيادية بالسعودية، شبكة الجزيرة الإعلامية، 2018، https://bit.ly/2UcC5zL

محمود، قاصد، جواد الحمد، عاطف الجولاني، عبد الحميد فخري، "الأزمة الخليجية 2017 البُعد الآخر، 2017، http://bit.ly/2OseJ7J.

مسار قرصنة وكالة الأنباء القطرية وصولا للإمارات، موسوعة الجزيرة الإلكترونية،2017، http://bit.ly/2nr0Hbc

سمو امير البلاد الشيخ صباح الأحمد: الأهم اننا اوقفنا الحل العسكري للازمة الخليجية، الحدث الإخبارية، الدقيقة 1:40، 2017، https://bit.ly/3kPM6yu

نائب مجلس الوزراء وزير الخارجية يجتمع مع الأمين العام لحلف شمال الأطلسي الناتو، وزارة الخارجية القطرية، 2019، https://bit.ly/38FTvh0

مسؤولة في الناتو: انضمام قطر إلى الحلف مهم جداً، صحيفة الشرق، 2018، https://bit.ly/3ltvIEj

مريم بومديان، وزير خارجية تركيا لـ الشرق: قطر طرف وازن في معادلة القوى الدولية لمواجهة الإرهاب، صحيفة الشرق، 2018، https://bit.ly/3eWX5o4

واشنطن: نعمل لإعلان قطر حليفاً رئيسياً من خارج الناتو.. وهذه المزايا التي ستحصل عليها، صحيفة الشرق، 2020، https://bit.ly/3ktOvOs

الوالي أحمد، خبير بشؤون "الأطلسي": هذه دلالات إعلان قطر حليفاً رئيساً للناتو، الخليج أونلاين، 2020، https://bit.ly/2GdJs6L

أحمد يوسف، قطر.. حليف رئيسي للناتو يسعى لعضوية كاملة، الانظول وكالة الانباء التركية، 2020، https://bit.ly/3eWssil

مايا أوتاراشفيلي، القرصنة الروسية ليست جديدة...الحرب الالكترونية الأولى في أستونيا، المجلة، 2017، https://bit.ly/3f2ymOX

بريطانيا وأميركا تساند جورجيا بتحميل روسيا مسؤولية استهدافها بهجمات إلكترونية، شبكة الجزيرة الإعلامية، 2020، https://bit.ly/38FpwFF

التهديدات الجديدة: الأبعاد الالكترونية، مجلة الناتو، حلف شمال الأطلسي (الناتو)، https://bit.ly/3kRTLfN

قطر.. مجلس الوزراء يوافق على إنشاء وكالة للأمن السيبراني، الخليج أونلاين، 2020، https://bit.ly/32ga0fy

وهوَ مركز مختص بتطوير وتعزيز القدرات السيبرانية لدى الناتو، كما يهتم بتطوير العقيدة والمفهوم، والوعي والتدريب، والبحث والتطوير، والتحليل والدروس المستفادة.

انخراط نشاط ونظام دفاعي حديث، تبناه قادة والحكومات في لشبونة "المفهوم الاستراتيجي للدفاع والأمن للدول الأعضاء في منظمة حلف شمال الأطلسي"، حلف شمال الأطلسي (الناتو)، 2010، https://bit.ly/3mJWUij

محمد الدوراني، قتال غير مرئي: الحرب السيبرانية في الأزمة الخليجية، مركز الجزيرة للدراسات، ترجمة: كريم الماجري، ص 9، 2018.

أحمد محمد بني عيسى، دور إدارة الازمات الالكترونية في حماية المنشئات الحيوية، دراسات أمنية استراتيجية، وزارة الداخلية القطرية، العدد الاول، ص 18، 2020.

المصادر الاجنبية

QATAR NATIONAL CYBER SECURITY STRATEGY, Qatar government, PP vi- vii, 2014, https://bit.ly/32kxjEW

Hassan, Shatha Zakary, "The Qatari Crisis and Its Impact on Gulf Relations & Journal of Law.", Political Sciences, 2018.

Jeffrey L.Caton, NATO cyberspace capability: a strategic and operation evolution, U.S. Army College, P2,2016, https://bit.ly/32rIGv0

NATO LEADERS CALL FOR GREATER COLLABORATION IN CYBERSPACE, Vigilia Pretium libertatis, NATO, https://bit.ly/3kc7LA1

Emilio Iasiello, Cyber Attack: A Dull Tool to Shape Foreign Policy, International Conference on Cyber Conflict, P2, 2013, https://bit.ly/3exmd4u

STEPHEN W. KORNS and JOSHUA E. KASTENBERG, Georgia's Cyber Left Hook, ARMY WAR COLLEGE CARLISLE BARRACKS PA STRATEGIC STUDIES INSTITUTE, P60, 2009, https://bit.ly/3n4eWvM

Vincent Joubert, Five years after Estonia's cyber attacks: lessons learned for NATO, Research Division, NATO Defense college, Rome, NO. 76, P1, 2012, https://www.files.ethz.ch/isn/143191/rp_76.pdf

Laura Brent, NATO'S role in cyberspace, NATO, 2019, https://bit.ly/2U16Qrk

Arkoon FAST360 A10, NATO, https://bit.ly/36volGr

What we do, NATO Communications and Information Agency (NCIA), https://bit.ly/3l4ZP4W

NATO's Cyber Security Centre, NATO Communications and Information Agency (NCIA), https://bit.ly/2I0upOV

Multinational Cyber Defence Capability Development (MN CD2), NATO Communications and Information Agency (NCIA), https://bit.ly/3exvYzv

NATO Cyber Defence, NATO, 2019, https://bit.ly/3mPRwu0

LILLIAN ABLON, ANIKA BINNENDIJK, QUENTIN E. HODGSON, BILYANA LILLY, SASHA ROMANOSKY, DAVID SENTY, JULIA A. THOMPSON, Operationalizing Cyberspace as a Military Domain, RAND corporation, P 8, 2019, https://bit.ly/3kW4yFU

Vincent Joubert, Five years after Estonia's cyber attacks: lessons learned for NATO, Research Division, P 4.

Z'hra M. Ghavam, NATO'S PREPAREDNESS FOR CYBERWAR, NAVAL POSTGRADUATE SCHOOL, p 44, 2016, https://bit.ly/32ocfxu

Neil robinson, Spending for success on cyber defence, NATO Review, 2017, https://bit.ly/3jYW4fX

What we do, NATO Communications and Information Agency (NCIA), https://bit.ly/3l4ZP4W

LILLIAN ABLON, ANIKA BINNENDIJK, QUENTIN E. HODGSON, BILYANA LILLY, SASHA ROMANOSKY, DAVID SENTY, JULIA A. THOMPSON, Operationalizing Cyberspace as a Military Domain, P 12.

Locked Shields, CCDCOE, The NATO Cooperative Cyber Defence Centre of Excellence, https://bit.ly/3p1RBgp

CYBER COALITION 16: NATOS LARGEST CYBER DEFENCE EXERCISE, Vigilia Pretium libertatis, NATO, https://bit.ly/3pa1rgc

NATO EXERCISE CYBER COALITION 17 UNDERWAY IN ESTONIA, Vigilia Pretium libertatis, NATO, https://bit.ly/32peKPW

Tallinn Manual 2.0, CCDCOE, The NATO Cooperative Cyber Defence Centre of Excellence, https://bit.ly/36bRw0R

JAMES A. LEWIS, THE ROLE OF OFFENSIVE CYBER OPERATIONS IN NATO'S COLLECTIVE DEFENCE, The Tallinn Papers, NO.8, P7, 2015, ***https://bit.ly/3n89rwp***