Security Policy Papers
أوراق السياسات الأمنية
https://spp.nauss.edu.sa/index.php/spp
https://nauss.edu.sa/
ورقة تحليل سياسات أمنية

تهديدات الأمن الإقليمي العربي في الميدان الخامس: نحو إستراتيجية للحماية

The Arab National Security Threats in the Fifth Domain: Towards a Strategy for Protection

إيهاب خليفة
مركز المستقبل للأبحاث والدراسات المتقدمة
الإمارات العربية المتحدة

Ehab Khalifa
Future for advanced research and studies
The United Arab Emirates

المخرجات الرئيسية:

- ضرورة وضع رؤية عربية موحدة، وإستراتيجية للتعامل مع الهجمات السيبرانية لما تشكله من تهديدات على أمن المنطقة، تعمل الدول العربية في إطارها، ويمكن أن يكون من خلال مجلس وزراء الداخلية العرب.
- التأكيد على أهمية التعاون الإستراتيجي بين دول المنطقة بمشاركة المعلومات والبيانات اللازمة لتحليل الأدلة الجنائية الرقمية Digital Evidence، التي تساعد على اكتشاف الهجمات السيبرانية فور حدوثها والعمل على تخفيف آثارها، وتتبع المعاملات المالية المقرصنة وكذلك العملات المشفرة، التي قد تستخدم في تمويل الحركات المتمردة والإرهابية.

المستخلص

مع تَوَجُّه العالم نحو الاعتماد المتزايد على التقنيات الذكية والحديثة وتَبَنِّي نماذج الحكومات والمدن الذكية، للاستفادة من مكتسبات الثورة الصناعية الرابعة في تحسين نمط الحياة البشرية، ومع تسريع عملية التحديث التكنولوجي التي تمر بها الدول والمجتمعات خاصة خلال فترة انتشار فيروس كوفيد 19- لضمان استمرار النشاط البشري العمراني أثناء الالتزام بتعليمات الحجر الصحي

Abstract

The world is moving towards increasing reliance on smart technologies throw adopting models of smart governments and smart cities, to get the gain of the Fourth Industrial Revolution in improving human lifestyle, and with accelerating the process of technological modernization that countries are going through, especially during the

والتباعد الاجتماعي، فقد أصبح العالم أجمع أكثر انكشافًا وعرضةً لمخاطر التهديدات السيبرانية.

ومع تزايد وتيرة الهجمات السيبرانية بصورة ملحوظة، وتزايد قدرتها التدميرية التي أصبحت قادرة على ضرب المفاعلات النووية والأقمار الاصطناعية، فضلًا عن البنية التحتية الحرجة، فإن ذلك يعني أن الحرب السيبرانية أصبحت أكثر احتمالًا من ذي قبل، بصورة قد تكون أكثر شراسة عن غيرها من الحروب، فخلال دقائق معدودة قد يقع آلاف من القتلى إذا نجحت هجمة سيبرانية في استهداف أحد المرافق الحيوية للدول كنظم الطيران أو المستشفيات.

ويعتبر الفضاء السيبراني هو ميدان المعركة الرئيس لهذه الجيوش السيبرانية، ولكنه ليس الميدان الوحيد، فكما تقاتل القوات المسلحة في الميادين الأربعة التقليدية (الأرض والبحر والجو والفضاء الخارجي)، فإن الجيوش السيبرانية تقاتل في جميع هذه الميادين مشتركة، إلى جانب قتالها أيضًا في الميدان الخامس الافتراضي وهو الفضاء السيبراني.

ومن هنا، تأتي أهمية هذه الورقة التي تناقش تهديدات الأمن الإقليمي العربي في الميدان الخامس، تلك التهديدات الجديدة الناجمة عن الاعتماد المتزايد على الفضاء الإلكتروني، وتسعى إلى تقديم رؤية تساعد متخذي القرار على صياغة إستراتيجية وطنية وعربية لمواجهة مخاطر التهديدات السيبرانية التي تواجه الأمن الإقليمي العربي السيبراني، تقوم على ثلاثة عناصر رئيسة، هي: ميدان المعركة القادم، والسلاح الملائم، والجيوش المقاتلة؛ فالميدان سيكون سيبرانيًّا، والسلاح سيكون برمجيًّا، والجيوش ستعمل من خلف الشاشات.

period of the spread of the Covid-19 virus, to ensure the continuation of human activity, while adhering to the instructions of quarantine and social distancing, the whole world has become more exposed to cyber threats.

With the noticeable increase in the frequency of cyber attacks, and the increasing destructive capacity that has become capable of striking nuclear reactors and satellites, as well as critical infrastructure, this means that cyber war has become more likely than before, in a way that may be more fierce than other wars, Within a few minutes, thousands of deaths may occur if a cyber attack succeeds in targeting one of the vital facilities of countries, such as aviation systems or hospitals.

Cyberspace is the main battlefield for this coming war. It is the fifth domain of the new battle after the four traditional fields - land, sea, air and outer space.

Hence the importance of this paper, which discusses threats to Arab regional security in the fifth domain, these new threats resulting from the increasing dependence on cyberspace, and seeks to provide a vision that helps decision makers in formulating a national and Arab strategy to confront the risks of cyber threats facing Arab regional cyber security.

مقدمة

مع تَوَجُّهِ العالم نحو الاعتماد المتزايد على التقنيات الذكية والحديثة، وتَبَنِّي نماذج الحكومات والمدن الذكية، للاستفادة من مكتسبات الثورة الصناعية الرابعة في تحسين نمط الحياة البشرية، ومع تسريع عملية التحديث التكنولوجي التي تمر بها الدول والمجتمعات، خاصة خلال فترة انتشار فيروس كوفيد 19- لضمان استمرار النشاط البشري العمراني أثناء الالتزام بتعليمات الحجر الصحي والتباعد الاجتماعي، فقد أصبح العالم أجمع أكثر انكشافًا وعرضة لمخاطر التهديدات السيبرانية؛ وذلك لأنه كلما زاد الاعتماد على الإنترنت في إدارة شؤون الحياة اليومية وتعددت الأهداف، التي يمكن أن تصبح جاذبة للقراصنة، ازدادت معها فرص الاختراقات والهجمات السيبرانية.

ومع تزايد وتيرة الهجمات السيبرانية بصورة ملحوظة، وتزايد قدرتها التدميرية التي أصبحت قادرة على ضرب المفاعلات النووية والأقمار الاصطناعية، فضلًا عن البنية التحتية الحرجة لمحطات الطاقة والوقود ونظم الاتصالات والمواصلات والمستشفيات وخلافه، فإن ذلك يعني أن الحرب السيبرانية أصبحت أكثر احتمالًا من ذي قبل، بصورة قد تكون أكثر شراسة عن غيرها من الحروب، فخلال دقائق معدودة قد يقع آلاف من القتلى إذا نجحت هجمة سيبرانية في استهداف أحد المرافق الحيوية للدول كنظم الطيران أو المستشفيات.

ويعتبر الفضاء السيبراني هو ميدان المعركة الرئيس لهذه الجيوش السيبرانية، ولكنه ليس الميدان الوحيد، فكما تقاتل القوات المسلحة في الميادين الأربعة التقليدية (الأرض والبحر والجو والفضاء الخارجي)، فإن الجيوش السيبرانية تقاتل في جميع هذه الميادين مشتركة، إلى جانب قتالها أيضًا في الميدان الخامس الافتراضي وهو الفضاء السيبراني.

ولأن السلاح المناسب لتحقيق الردع وحفظ الأمن يكون من مشتقات عصره؛ حتى يكون فعالًا ومناسبًا، فالسلاح هنا يجب أن يكون سيبرانيًّا وذكيًّا، يختلف عن الأسلحة التقليدية الأخرى، فمثلًا حينما كان المجتمع البشري زراعيًّا كانت الْحِرَاب والرماح والسيوف، وجميعها أسلحة من موارد الأرض مباشرة وبتدخل طفيف من الإنسان عليها، وحينما فرض الإنسان مزيدًا من السيطرة على الطبيعة وأصبح المجتمع صناعيًّا استطاع تطوير الدبابات والطائرات وغيرها من الأسلحة، وحينما يصبح المجتمع «ذكيًّا» فإن السلاح يجب أن يساير هذا العصر الجديد، وإلا فلن يكون فعّالًا في حفظ أمن الدولة وأهدافها.

ومن هنا تأتي أهمية هذه الورقة التي تناقش تهديدات الأمن الإقليمي العربي في الميدان الخامس، تلك التهديدات الجديدة الناجمة عن الاعتماد المتزايد على الفضاء الإلكتروني، وتسعى إلى تقديم رؤية تساعد متخذي القرار على صياغة إستراتيجية وطنية وعربية لمواجهة مخاطر التهديدات السيبرانية، التي تواجه الأمن الإقليمي العربي السيبراني، وتقوم على ثلاثة عناصر رئيسة، هي: ميدان المعركة القادم، والسلاح الملائم، والجيوش المقاتلة؛ فالميدان سيكون سيبرانيًّا، والسلاح سيكون برمجيًّا، والجيوش ستعمل من خلف الشاشات.

أولًا: الجدل النظريّ حول طبيعة التهديدات السيبرانية:

يعتبر «الأمن السيبراني» أحد عناصر الأمن الوطني غير التقليدية؛ وذلك لأنه يستطيع أحد مستخدمي الفضاء الإلكتروني أن يوقع خسائر

فادحة بالطرف الآخر، وأن يتسبب في شَلِّ البنية المعلوماتية والاتصالاتية الخاصة به، وهو ما يسبب خسائر عسكرية واقتصادية فادحة، من خلال قطع أنظمة الاتصال بين الوحدات العسكرية بعضها البعض أو تضليل معلوماتها أو سرقة معلومات سرية عنها، أو من خلال التلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسيب، أو السيطرة على نظم الذكاء الاصطناعي وإنترنت الأشياء، أو اختراق أسراب من الدرونز أو الربوتات أو السيارات ذاتية القيادة وتوجيهها للقيام بأعمال تخريبية، وبالرغم من فداحة الخسائر إلا أن الأسلحة بسيطة، فهي عبارة عن برمجيات لا تتعدى كيلوبايت، تتمثل في فيروسات تخترق شبكة الحاسوب وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاية عالية، وهي في ذلك لا تُفَرِّق بين المقاتل والمدني، وبين العام والخاص، وبين السري والمعلوم.

وتتعدد تعريفات الأمن السيبراني، فهناك من يقوم بتوسيعها؛ لكي تُعَبِّر عن القدرة على حماية بيانات الدولة وشبكاتها، مثل: تعريف Lewis, J. A بأنه «حماية شبكات الحاسوب والمعلومات التي تحتويها من الاختراق أو التدمير أو الاضطرابات الضارة» (Lewis, 2006)، أو تعريف الأمن الإلكتروني بأنه «القدرة على حماية أو الدفاع عن استخدام الفضاء السيبراني من الهجمات السيبرانية» (Committee on national security systems, 2015)، أو هو «فن ضمان وجود واستمرارية مجتمع المعلومات في دولة ما، وضمان وحماية المعلومات والأصول والبنية التحتية الحيوية في الفضاء الإلكتروني» (Canongia & Mandarino, 2014).

ومن التعريفات من يُحَدِّد إجراءات وسياسات الأمن السيبراني، مثل: تعريف الاتحاد الدولي للاتصالات له بأنه «مجموع الأدوات والسياسات والمفاهيم الأمنية والضمانات والمبادئ ومناهج إدارة المخاطر والإجراءات والتدريبات وأفضل الممارسات والضمانات التكنولوجية، التي يمكن استخدامها لحماية البيئة السيبرانية والمستخدم والمنظمة بصورة عامة» (Cybersecurity guide for developing countries, 2009). كما يُعرف الأمن السيبراني أيضًا بأنه عملية «الحد من خطر الهجمات الضارة على برامج وأجهزة الحاسوب والشبكات، من خلال استخدام أدوات كشف الاختراقات، ووقف نشاط الفيروسات، ومنع الدخول غير المصرح به، وتأكيد الهويات، وتمكين الاتصالات المشفرة» (Craigen et al.,2014)، وهو أيضًا «مجموعة من التقنيات والعمليات والممارسات والاستجابات وتدابير الحد من المخاطر المصممة لحماية الشبكات والحواسيب والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به من أجل ضمان السرية والنزاهة والإتاحة» (Government of Canada, 2010)، كما تُعَرِّفه أيضًا وزارة الداخلية الأمريكية بأنه «النشاط أو العملية، أو القدرة أو الإمكانية، أو الحالة التي يمكن من خلالها حماية المعلومات ونظم الاتصالات والدفاع عنها من الضرر أو التعديل أو التجسس أو التدمير أو الدخول غير المصرح به» (National Initiative for Cybersecurity Careers and Studies, 2021).

ثانيًا: الاستعداد لجيل جديد من التهديدات السيبرانية أكثر عنفًا وأوسع انتشارًا:

تميزت الهجمات السيبرانية خلال العقد الماضي بكونها هجمات محدودة ومؤقتة، لا تؤثر في قطاع كبير من المستخدمين، ولا تتسبب في شلل الإنترنت أو وقف

الخدمات الحكومية بصورة كبيرة، وباستثناء الهجمات التي لها طابع عسكري، مثل: «ستاكس نت»، فقد اقتصرت هذه الهجمات على استهداف الحسابات البنكية واختراق المواقع الإلكترونية والصفحات الرسمية على مواقع التواصل الاجتماعي، وعادة ما كانت تتسبب هذه الهجمات في شلل مؤقت للخدمة يتم تلافيه بسرعة من قبل الفنيين والمختصين.

لكن منذ بداية العقد الحالي، بدأت الهجمات السيبرانية تأخذ أبعادًا مختلفة أكثر تطورًا وخطورة، مدفوعة في ذلك بحالة التحديث التكنولوجي غير المسبوقة التي شهدتها الدول بصورة عامة والمنطقة العربية بصورة خاصة خلال فترة انتشار فيروس كوفيد19-، فتم استهداف أكبر محطات الطاقة وشركات الإمداد والتموين حول العالم ببرمجيات الفدية، وأصبحت البنى التحتية الحرجة، مثل: السدود ومحطات الطاقة والمستشفيات أكثر تأثرًا بمخاطر التهديدات السيبرانية.

ولم يكن غريبًا أن تجمع قمة غير عادية، في يونيو 2021م، بين الرئيس الأمريكي جو بايدن والرئيس الروسي فلاديمير بوتين في سويسرا حيث تم فيها مناقشة قضية التهديدات السيبرانية باعتبارها أكثر القضايا الحرجة أهمية على المستوى القومي (القرصنة الإلكترونية، 2021).

ولذلك يمكن القول، إن الجيل الجديد من الهجمات السيبرانية يتميز بخصائص أكثر تعقيدًا وعنفًا عما سبقه، وذلك لعدة أسباب منها:

- سرعة تطور شكل الهجمات السيبرانية: في هذا الجيل يتطور شكل الهجمات السيبرانية بصورة سريعة، فقد يكون عبر أجهزة الحاسوب، أو إنترنت الأشياء، أو أجهزة الهواتف المحمولة، وقريبًا قد يكون عبر نظم الذكاء الاصطناعي والروبوت، وقد يستهدف الأموال، أو الاعتراض السياسي، أو الإرهاب، أو العنف غير المبرر.
- ضيق الفجوة الزمنية بين الهجمات الكبرى: فيكون الفارق الزمني بين هجمة سيبرانية وغيرها قصيرًا جدًّا، فتحدث عدة هجمات كبرى خلال عام واحد، فما يكاد العالم يخرج من تداعيات هجمة حتى تظهر له غيرها، وتكون مختلفة في الآلية والنطاق والجمهور.
- زيادة درجة تعقيد الهجمة وتداعياتها: فأصبحت الهجمات معقدة في طريقة تنفيذها، ويصعب تعقبها أو معرفة مصدرها، ويشارك فيها عدد كبير من الأفراد حول العالم، وتستخدم أجهزة غير متوقعة في عملية القرصنة، مثل: الطائرات دون طيار من أجل التضليل، وتكون تداعياتها لا تُحتمل سواء أكان ذلك على مستوى الأفراد أم الدول.
- دور بارز للفواعل من غير الدول: يلعب الفواعل من دون الدول دور مهم في الهجمات السيبرانية، قد يكون مساويًا لدور الدول، سواء أكانت مجموعة قرصنة أم حركات إرهابية أم مافيا دولية، أم أفراد عاديين، كما يتم تطوير العديد من برامج القرصنة التي لا تحتاج إلى مطورين ومختصين لاستخدامها، بل يمكن شراؤها واستخدامها بصورة سهلة، وهو ما يفتح الباب لقطاع كبير من غير المختصين للمشاركة في هذا النوع من الهجمات.
- تصاعد خطورة نمط هجمات الفدية: خلال عام كورونا، تطور شكل هجمات برامج الفدية، فأصبحت ذات ضرر مزدوج، بحيث يقوم المهاجمون بتشفير كميات كبيرة من بيانات الضحية بهدف الابتزاز والحصول على الأموال،

وبعد قيام الضحية بدفع الأموال لفتك تشفير البيانات، يقوم القراصنة بابتزازه مرة أخرى حتى لا يتم تسريب هذه البيانات، كما لاحظ الباحثون أن الجيل الجديد من برمجيات الفدية يقوم بتشفير كل 16 بايت من الملف المصاب، وهو ما يعني أن بعض حلول حماية برامج الفدية لا تلاحظ ذلك؛ لأن «المستند المشفر يبدو إحصائيًّا مشابهًا جدًّا للنسخة الأصلية غير المشفرة»، وبذلك فهي طريقة تشفير جديدة مبتكرة لم يتم ملاحظتها من قبل.

- الاعتماد على العملات المشفرة: مثل البيتكوين؛ وذلك لأنها صعبة التعقب، وليس لها إدارة مركزية، ومع ذلك يمكن البيع والشراء من خلالها، فأصبحت العملة الرسمية للهجمات السيبرانية، وبصورة خاصة هجمات الفدية التي باتت أكثر انتشارًا من ذي قبل.

ونتيجة لذلك، فقد رصدت شركات الأمن السيبراني، خلال عام 2020م، حالة التصعيد السيبراني غير المسبوق على مستوى العالم، فتم رصد حملة سيبرانية تستهدف التجسس على الحكومات والقوات المسلحة شملت أكثر من 1093 هدفًا في 27 دولة حول العالم، من بينهم إيران وأفغانستان والهند وباكستان وألمانيا (The hindu business line, 2020)، كما تزايد نشاط مجموعات القرصنة القومية المدعومة من الحكومات، مثل: روسيا والصين وكوريا الشمالية، خاصة ضد أوروبا والولايات المتحدة الأمريكية، سواء أكان ذلك لأسباب سياسية تتعلق بالانتخابات الأمريكية أو فرض السيطرة والنفوذ على شرق أوروبا أم لأسباب اقتصادية واستخباراتية أخرى (Newman, 2021)، ومن ناحية أخرى، تعرضت الولايات المتحدة الأمريكية لأكبر اختراق أمني وأسوئه على الإطلاق، الذي نجم عنه اختراق وزارة الخزانة والتجارة وغيرها من المؤسسات الفيدرالية (Jibilian, 2021)، وتعطي جميع هذه التطورات مؤشرًا عن الطبيعة الجديدة للهجمات السيبرانية، التي أصبحت أكثر عنفًا وخطورة من ذي قبل.

ثالثًا: المخاطر والتهديدات السيبرانية التي تؤثر في الأمن العربي:

على الرغم من تَوَجُّه كثير من دول المنطقة العربية نحو تبني إستراتيجيات للأمن السيبراني وبناء مؤسسات وظيفتها تحقيق الأمن الوطني السيبراني، إلا أن ذلك لم يمنع وقوع عدة تهديدات سيبرانية كبرى، وذلك لعدة أسباب؛ فمن ناحية شهدت دول منطقة الشرق الأوسط تحولًا ملحوظًا نحو التوسع في البنية التحتية الرقمية خلال السنوات القليلة الماضية، الأمر الذي جعلها جاذبة لعمل القراصنة والعصابات الإجرامية، التي تستغل ضعف الثقافة الرقمية لدى كثير من شعوب المنطقة، ومن ناحية أخرى، تظهر أحيانًا بعض الخلافات بين دول المنطقة، والتي تتحول إلى هجمات سيبرانية، على سبيل المثال: بعض الهجمات السيبرانية التي شنتها إيران، كنوع من التهديد السيبراني للأمن العربي، ونجم عنها في بعض الأحيان تأثر إمدادات النفط إلى الأسواق العالمية، هذا إلى جانب عمل الجماعات الإرهابية التي حاولت استغلال الفضاء السيبراني لأغراض التمويل أو التجنيد في المنطقة العربية، وهو ما جعل الإنترنت أحد مصادر التهديد المباشرة في المنطقة العربية.

ووفقًا لمؤشر الأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات عام 2020م، فإن أربع دول عربية فقط جاءت ضمن أول 50 مرتبة في مؤشر الأمن السيبراني،

وهم على الترتيب: المملكة العربية السعودية التي جاءت في المرتبة الثانية عالميًا، والإمارات العربية المتحدة التي جاءت في المرتبة الخامسة، وسلطنة عمان التي جاءت في المرتبة الحادية والعشرين، وجمهورية مصر العربية التي استحوذت على المرتبة الثالثة والعشرين، ودولة قطر التي جاءت في المرتبة السابعة والعشرين (International Telecommunication Union, 2020)، وبذلك يعكس هذا المؤشر حالة عدم التجانس الإقليمي من حيث الأمن السيبراني، فبينما تستحوذ السعودية والإمارات على مرتبة متقدمة في مجال الأمن السيبراني، تأتي عمان ومصر وقطر في مرتبة متوسطة، يليها البحرين والكويت والأردن ولبنان وبقية الدول العربية.

وفي هذا الإطار، يمكن تحديد بعض أوجه الخطر التي باتت تؤثر بصورة مباشرة في الأمن الإقليمي العربي في الميدان الخامس، التي منها:

- استهداف البنية التحتية الحرجة للدولة: إذ يتم استهداف البنية التحتية للدولة، سواء أكانت مدنية أم عسكرية بهجمات سيبرانية، مثل: استهداف محطات الطاقة والوقود والخدمات المالية والمصرفية ونظم الاتصالات والمواصلات، ومن الأمثلة على ذلك: قيام إيران عام 2012م بشن هجمة سيبرانية على شركة النفط السعودية «أرامكو»، التي أسفرت عن تعطيل حوالي 30 ألف جهاز حاسوب؛ لتصبح بذلك هذه العملية من بين أكثر الهجمات تدميرًا (لوديرميلك، 2019)، ثم عاودت الكرة مرة أخرى عام 2016م وشنت هجومًا سيبرانيًا على أجهزة الحاسوب في البنك المركزي السعودي ووزارة النقل والوكالة المختصة بإدارة مطارات السعودية، وتسببت الهجمة في مسح كميات كبيرة من البيانات، إلا أن الوكالات السعودية استطاعت استعادتها من النسخ الاحتياطية.
- جمع معلومات اقتصادية استخباراتية: وهو ما يتحقق عن طريق اختراق قواعد البيانات المالية والمصرفية وقواعد بيانات الشركات والبنوك وجمع المعلومات، التي قد تؤثر في الأمن القومي للدولة، وكذلك من خلال التجسس على المسؤولين الماليين ووزراء المالية ورؤساء الشركات الكبرى.
- السيطرة على الأنظمة العسكرية: من خلال قيام قراصنة محترفين أو جيوش نظامية سيبرانية بشن هجمات بغرض السيطرة على نظم القيادة والسيطرة عن بعد، الأمر الذي يؤدي إلى إخراج بعض منظومات الأسلحة عن سيطرة القيادة المركزية، وإعادة توجيهها نحو أهداف داخلية أو ضد دول صديقة، كما يمكن أيضًا السيطرة على الطائرات دون طيار، أو الغواصات في أعماق البحار، أو السيطرة على الأقمار الاصطناعية العسكرية في الفضاء الخارجي وإخراجها عن سيطرة الدولة التابعة لها.
- سرقة المعلومات والبيانات العسكرية أو التلاعب بها: من خلال اختراق قواعد البيانات العسكرية وسرقتها أو تزييفها أو تدميرها إلكترونيًا، حيث تسعى الهجمات السيبرانية، في هذه الحالة، إلى اختراق الشبكات الخاصة بالمؤسسات العسكرية بهدف سرقة أو تدمير أو تزييف خرائط نشر أنظمة التسليح أو التصميمات الخاصة بالمعدات العسكرية أو مناطق انتشار القوات أو أي معلومات تتعلق بالقوات المسلحة.
- اختراق أجهزة إنترنت الأشياء: تنتشر أجهزة إنترنت الأشياء Internet of things وأجهزة الاستشعارات Sensors في المجتمعات الذكية بصورة كبيرة، داخل المؤسسات والشركات والمنازل

والمطاعم والمقاهي بل الشوارع أيضًا، وهذا يعني إنشاء جيش عملاق من مليارات الأجهزة ضعيفة التأمين، سهلة الاختراق، وتكون منتشرة في كل الأماكن، وجميعها متصل بالإنترنت، فإذا تم اختراق هذه الأجهزة والسيطرة عليها، وحقنها بالفيروسات والديدان وأحصنة طروادة، فإنها ستتحول مباشرة إلى جيش مسلح قادر على تدمير البنية التحتية الحرجة كالبنوك ومحطات الطاقة والسدود والمستشفيات وقطاع الاتصالات، أو حتى تعطيل الخدمات المالية والمصرفية ووقف جميع الخدمات الحكومية، بل يمكن أن يتسبب ذلك في تدمير شبكة الإنترنت نفسها (Eastwood, 2017).

- السيطرة على نظم الذكاء الاصطناعي: تعتمد المجتمعات الذكية على تقنيات الذكاء الاصطناعي، مثل: نظم الروبوتكس Robotics في المصانع والشركات والمحال التجارية، ونظم الرد الآلي على العملاء، وأيضًا السيارات ذاتية القيادة والطائرات دون طيار، فإذا تم اختراق هذه النظم، فسنجد جيوشًا من السيارات ذاتية القيادة تسير في الشوارع وتقتل الأفراد دون معرفة الجاني الحقيقي المتسبب في ذلك، كما يمكن نظريًّا أيضًا السيطرة على جيوش من الطائرات دون طيار والروبوتات وإعادة توجيهها؛ لتقوم بمهام القتل والتدمير، بصورة تجعل محاولة اختراق هذه النظم من أخطر التهديدات التكنولوجية التي يمكن أن يتعرض لها البشر (The new eyes of surveillance, 2014).

رابعًا: آليات التعامل مع التهديدات السيبرانية على المستوى الوطني:

إن التعامل مع التهديدات السيبرانية يتطلب مراعاة طبيعتها الخاصة من حيث الفاعلين فيها وميدان المعركة ونوعية الخسائر؛ فالفواعل قد تكون من الدول أو من غير الدول، مثل: جماعات القرصنة التي تشارك الحرب إلى جوار الدولة، أما ميدان المعركة فهو بيئة مصنوعة وليست طبيعية تحكمها قواعد الطبيعة، ولا يستطيع القانون الدولي أن يحكم التفاعلات التي تجري فيها، ليس فقط لغياب مفهوم السيادة فيها، ولكن لصعوبة معرفة الفاعل الحقيقي الذي قام بشن هذه الهجمات السيبرانية على الطرف الآخر أيضًا، والخسائر فيها قد تكون مباشرة تتمثل في تدمير البيانات والبنى التحتية والمعدات العسكرية، وقد تكون غير مباشرة تتمثل في تراجع التنافسية الاقتصادية للدولة وفقدان الثقة في الاقتصاد الوطني بسبب الهجمات السيبرانية، التي تستهدف المؤسسات المالية والتجارية والصناعية (خليفة، 2021).

ولكي يمكن التعامل مع التهديدات السيبرانية وتخفيف وطأتها على الأمن الوطني والإقليمي يجب إدراك الطبيعة الخاصة بالميدان الخامس، التي تتمثل في الآتي:

- محورية دور الفضاء السيبراني في إدارة شؤون الحياة اليومية:

أصبح الفضاء السيبراني عصب الحياة البشرية وشريانها ومصدر طاقتها وترابطها؛ فإدارة نظم الاتصالات والمواصلات ومحطات الكهرباء والمفاعلات النووية والسدود والخزانات، والتحكم في إشارات المرور واتجاه الطرقات والجسور، وتسيير حركة السيارات ذاتية القيادة والدرونز، وإجراء عمليات تحويل الأموال والبيع والشراء، جميعها تتم بتكنولوجيات مرتبطة بشبكات الحاسوب والإنترنت، فالحياة البشرية تقريبًا قد هاجرت من الأرض، ولكن ليس إلى المريخ كما في أفلام الخيال العلمي، بل إلى

الفضاء السيبراني، وهنا يجب إدراك أن استهداف مصالح الدول في ذلك الميدان الخامس هو بمثابة حالة حرب حقيقية ضدها.

- طبيعة البيئة السيبرانية باعتبارها بيئة صناعية وليست طبيعية:

يختلف الميدان الخامس - الفضاء السيبراني- عن غيره من الميادين التقليدية الأخرى، كالأرض والبحر والجو والفضاء، فهو ميدان صناعي وليس طبيعي، لا تحكمه قوانين الطبيعة والجاذبية، بقدر ما تحكمه بروتوكولات تدفق البيانات عبر الأسلاك وبين الأجهزة وفي الموجات الهوائية، وبالتالي، فإن الطائرات والدبابات والصواريخ لن تجدي نفعًا داخل هذا الميدان، ولن تساوي قيمتها الحقيقية سنتًا واحدًا في حرب سيبرانية كبيرة، وهو ما يفرض على الدول، التي تسعى إلى الحفاظ على أمنها، أن تُطَوِّرَ السلاح المناسب والفعّال والقابل للاستخدام في هذا الميدان الجديد.

- صعوبة الاعتماد على الآخرين لتحقيق الأمن السيبراني:

إذا كانت الدول ضعيفة ومتوسطة القوة تستورد الأسلحة من الدول العظمى؛ لتحقق بها انتصاراتها العسكرية، فإن ذلك لن يجدي نفعًا مع النوع الجديد من الحروب، فعلى عكس البندقية التي يحملها العسكري ويتحكم فيها كيفما يشاء، فإن التكنولوجيات المستوردة من الخارج قد تكون مخترقة، ويمكن التحكم فيها عن بُعْد وتعطيلها في حال رَغِبَ صانعها في ذلك، وهو ما يضع تحديًا آخر أمام الدول؛ لكي تطور سلاحها بنفسها داخل هذا الميدان، حتى لا تقع ضحية في حال قرر الأصدقاء التخلي عنها لصالح أعدائها.

- عدم القدرة على تحقيق الردع في الفضاء السيبراني:

الردع، بصفة عامة، هو منع الخصم من القيام بفعل عدائي، إما بسبب تخوفه من هجوم مضاد يفوق قدراته الدفاعية، أو بسبب ارتفاع تكلفة الهجوم مقارنة بالمكاسب التي يمكن أن يحققها (Trujillo, 2014)، ويعتبر الردع النووي هو النموذج التقليدي لفهم حالة الردع في العلاقات الدولية، إلا أن ذلك لا ينطبق على الفضاء السيبراني، حيث يتميز بعدم وجود حدود جغرافية له توضح سيادة الدول عليها، ولما كانت الأسلحة المستخدمة في الفضاء السيبراني هي أسلحة غير محددة سلفًا وتخضع للتطور التكنولوجي، وغالبًا ما تظهر نتيجة الثغرات الصفرية أو الفيروسات التي يتم تطويرها- فإنه يصعب حصر هذه الأسلحة لمنع أو تقنين استخدامها (Metzger, 2015)، فضلًا عن صعوبة معرفة الطرف المعتدي أو الذي قام بالهجوم السيبراني من الأساس، وذلك بسبب الطبيعة المعقدة والمتداخلة للهجمات السيبرانية، فإن تحقيق الردع عبر الفضاء السيبراني أمر غير ممكن بالمفهوم التقليدي.

وبالتالي، فإن الاستعداد للمعركة السيبرانية القادمة يتطلب من الدول بذل كثيرٍ من الجهد على مستوى التعليم والتطوير والتدريب، فلا يمكن تحقيق النصر عبر الفضاء السيبراني من خلال استيراد كافة أنواع التقنيات الذكية من الخارج، التي قد تحتوي على أبواب خلفية وثغرات يمكن إساءة استغلالها في وقت الحرب، ويجب على الدول التي تسعى إلى تحقيق النصر في هذه المعركة القادمة أن تبني قواتها المسلحة السيبرانية بقدراتها الذكية، دون الاعتماد الكامل على الاستيراد من الخارج مثلما

يحدث مع الأسلحة التقليدية، بالإضافة إلى تشكيل تحالفات سيبرانية إقليمية تسهم في تحقيق الأمن الإقليمي السيبراني.

ومن هنا، فإن الحفاظ على الأمن الوطني عبر الفضاء السيبراني يتطلب من الدول العمل من خلال عدة محاور رئيسة، هي:

- بناء القدرات السيبرانية الوطنية:

عبر تعليم الأطفال في مرحلة الصغر تطبيقات البرمجة، والتوسع في معاهد وكليات الذكاء الاصطناعي، وتبني الموهوبين من الطلاب في مجال الحاسوب ودمجهم في صفوف القوات المسلحة، ودعم الشركات الوطنية الناشئة التي تعمل في مجال الأمن السيبراني والحماية السيبرانية، ووضع القواعد القانونية والتشريعية التي تضمن الحفاظ على بيئة سيبرانية صحية داخل الدولة تقلل مخاطر الاختراق السيبراني الخارجي، وتضع معايير صارمة على المؤسسات والجهات الحيوية بالدولة، وتساعد الشركات والمؤسسات المالية على الحفاظ على أصولها من الاختراق أو التسريب، وتضع حدًّا لتجاوزات القراصنة والمنظمات الإجرامية والجماعات الإرهابية من التلاعب بالبنية التحتية للدولة.

- تطوير منظومة أسلحة سيبرانية وطنية:

يجب أن تعمل الدول جاهدة على بناء منظومة أسلحتها السيبرانية بنفسها، تلك الأسلحة التي تستخدمها للقتال عبر الفضاء السيبراني من الفيروسات والديدان والبرمجيات الذكية، فضلًا عن تجنيد محترفي القرصنة والبرمجة في صفوف القوات المسلحة التقليدية؛ لكي يشكلوا جيوشًا سيبرانية تمثل ذراعًا أساسية للمساهمة في تحقيق الأمن الوطني، ويصبحوا بمثابة «جنود ظل» يعملون خلف شاشات الحاسوب، ولديهم من الإمكانات والتقنيات البرمجية والإلكترونية ما يمكنهم من تغيير قواعد اللعبة في أوقات الأزمات والحروب، فيصبحوا هم عماد إدارة الصراعات العسكرية.

- تكوين أحلاف سيبرانية إقليمية:

وذلك من خلال إنشاء أحلاف سيبرانية جديدة أو تطوير مواثيق المنظمات الإقليمية التقليدية؛ لكي تشمل أيضًا التصدي للتهديدات السيبرانية، تمامًا مثل: حلف الناتو، بما يساعد على تبادل المعلومات بين المؤسسات الأمنية الإقليمية حول الهجمات السيبرانية ذات الطبيعة المعقدة، وتكوين درع إقليمي يسهم في صَدّ التهديدات السيبرانية عن دول الجوار الإقليمي.

- إنشاء وحدات سيبرانية عسكرية:

اتجهت كثير من دول العالم إلى إنشاء جيوش سيبرانية وفرق للعمليات عبر الفضاء السيبراني داخل صفوف قواتها المسلحة، وتتكون من قراصنة معلومات مهمتهم اختراق شبكات الحاسوب الخاصة بالخصم، ونشر برامج التجسس والمراقبة، وتنفيذ المهمات العسكرية التي تُطْلَب منها كتعطيل أحد البرامج العسكرية للخصم أو السيطرة على إحدى الشبكات أو تدمير بعض الخدمات الإلكترونية، فضلًا عن الدفاع عن الشبكات الوطنية وحمايتها من أي محاولة اختراق (خليفة، 2021).

وتتمثل مهمة الجيوش السيبرانية، في وقت السلم، في تقديم الدعم المعلوماتي واللوجستي؛ فيقومون بالتجسس على العدو عبر اختراق شبكاته؛ لكشف أسراره وسرقة تصميمات الأسلحة المتقدمة التي يمتلكها والخطط الإستراتيجية والاقتصادية في حالة الحرب، ومعرفة نوع التسليح الذي يمتلكه

ومناطق توزيعه وانتشاره، والأهداف التي يسعى إلى تدميرها في حالة الحرب، ومناطق تمركز القوات وعدد أفرادها ومواعيد نومهم ونشاطهم والوجبات التي يأكلونها بل المتعاقد الذي يُوَرِّد لهم هذه الوجبات، فكل معلومة في وقت الحرب قد تفيد في الإيقاع بالخصم.

وفي وقت الحرب، تقوم بمهمتي الهجوم والدفاع على حد سواء، فضلًا عن مهمة تقديم الدعم للوحدات العسكرية المقاتلة في الميادين المختلفة، فيقومون بمهمة الهجوم من خلال محاولة شن هجمات سيبرانية تستهدف نظم التحكم والسيطرة الخاصة بالعدو من خلال تعطيل نظم الدفاع الجوي، ومنصات إطلاق الصواريخ، والسيطرة على الأسلحة ذاتية التشغيل كالدرونز Drones والربوتات العسكرية، وقطع شبكات الاتصال بين الوحدات العسكرية، فضلًا عن القيام بعمليات الخداع والتشويش الرقمي على أجهزة العدو، ومن ناحية أخرى، هم مسؤولون عن الدفاع من خلال تأمين الاتصالات بين الوحدات العسكرية الصديقة المقاتلة، ومنع أي محاولات لاختراقها أو التجسس عليها، ويقومون بدور الضامن لسلامة وسهولة التواصل بين الوحدات المقاتلة، وتأمين القوات العسكرية خلف خطوط العدو عبر تعطيل نُظُمِهِ العسكرية وكشف الكمائن التي ينصبها لهم.

خامسًا: التجارب الدولية في مجال التعاون الإقليمي لمكافحة التهديدات السيبرانية: الناتو نموذجًا:

تكمن أهمية الفضاء السيبراني، بالنسبة لحلف الناتو، ليس فقط في دعم العمليات العسكرية التي يقوم بها الحلف في مناطق الصراع، لكن الحلف يعتبر نفسه أيضًا مسؤولًا عن تأمين مليار نسمة تقريبًا، يمثلون تعداد الدول الأعضاء في دول الحلف، سواء من التهديدات الناجمة عن الفضاء السيبراني، أو من التقنيات الحديثة بصورة عامة، مثل: الجيل الخامس للاتصالات G5، والدرونز، والطابعات ثلاثية الأبعاد، التي يمكن أن تُهدد أمن وسلامة المدنيين والعسكريين على حد سواء. من هنا، أصبح مفهوم الدفاع السيبراني عنصرًا أساسيًّا ضمن عناصر الدفاع الجماعي، واحتل الفضاء السيبراني مكانة مهمة في العقيدة العسكرية للحلف.

وإدراكًا من الناتو لطبيعة وخطورة التهديدات السيبراني، فقد قامت الدول الأعضاء عام 2014م بتوقيع سياسة الناتو للدفاع السيبراني NATO Policy on Cyber Defence، وقد تم إجراء تعديلات جديدة عليها في فبراير 2017م لضمان حوكمة تطبيق هذا المفهوم داخل المؤسسات المعنية بالدفاع داخل الحلف ووضع أطر محددة لمفهوم الدفاع السيبراني لدمجه في عمليات التخطيط والتشغيل سواء أكان ذلك على المستوى المدني أم العسكري، وبهذا أصبح الدفاع السيبراني في قلب مهام الدفاع الجماعي لحلف الناتو بهدف حماية الشبكات الخاصة بالدول الأعضاء من الهجمات السيبرانية سواء أكانت على الشبكات العسكرية أم المدنية؛ ليصبح من حق الأعضاء المطالبة بتطبيق المادة الخامسة من المعاهدة التأسيسية في حالة تعرضهم لهجوم سيبراني (Cyber defence, 2019).

ويشمل مفهوم الدفاع السيبراني عند الناتو حماية شبكات الحلف من الهجمات السيبرانية وتحقيق الأمن السيبراني للدول الأعضاء، وكذلك توظيف القوة السيبرانية المطلوبة للمساعدة على تنفيذ العمليات والمهام العسكرية، فضلًا عن تبني مفهوم الدفاع السيبراني الوقائي أو الإيجابي Positive Cyber Defence الذي يعني منع

الهجمة قبل حدوثها من خلال اتخاذ تدابير وقائية أو هجمات سيبرانية استباقية؛ أي ضرب مصدر التهديد المحتمل منعًا لشن هجمات سيبرانية، وبالتالي قيام الحلف بشن هجمات سيبرانية وقائية على مصادر التهديد؛ لمنعها مستقبلًا من شن عمليات عسكرية ضد الحلف وأعضائه.

وفي قمة وارسو عام 2016م أصدر الناتو تفويضًا دفاعيًّا يعتبر الفضاء السيبراني بمثابة ميدان للعمليات العسكرية، وأن الحلف يجب أن يحقق الأمن داخل هذا الميدان مثلما يحققه في الميادين التقليدية الأخرى، واعتبر أن قواعد القانون الدولي تنطبق على الفضاء السيبراني، وأن الحق في استخدام القوة في الدفاع عن النفس ينطبق أيضًا على القوة السيبرانية المتمثلة في شن الهجمات السيبرانية على دول الحلف، وأصدر في ذلك «دليل تالين» الذي يعتبر المرجع القانوني للناتو في الحروب السيبرانية، وفي العام نفسه أيضًا وَقَّعَ أعضاء الحلف تعهدًا بزيادة القدرات الدفاعية السيبرانية لهم، وخصص الحلف موارد للتعليم والتدريب في مجال الأمن السيبراني، وتعهد الحلفاء أيضًا بتعزيز الدفاعات السيبرانية للشبكات والبنية التحتية الوطنية وتعزيزها، وجعل ذلك بمثابة أولوية قصوى، إلى جانب التطوير المستمر لقدرات الناتو الدفاعية، كجزء من التكيف طويل المدى للناتو؛ لأن ذلك يعزز الدفاع السيبراني والمرونة الشاملة للحلف (Warsaw summit communique, 2016).

كما قام الناتو بإنشاء عدد من المؤسسات والفرق المعنية بالاستجابة السريعة لطوارئ الحاسوب، التي تعمل على مدار الساعة واليوم دون توقف بهدف تقديم الدعم الفني واللوجستي لأعضاء الحلف لمواجهة الهجمات السيبرانية، مثل: فريق الاستجابة السريعة لطوارئ السايبر Cyber Rapid Reaction Teams ووكالة الناتو للاتصالات والمعلومات NCI Agency في بلجيكا، وإنشاء مركز التميز للدفاع السيبراني التعاوني CCDCOE في تالين بإستونيا (Cyber defence, 2019).

سادسًا: نحو صياغة إستراتيجية عربية مشتركة للأمن الإقليمي السيبراني:

إن غياب رؤية عربية موحدة وإستراتيجية للتعامل مع الهجمات السيبرانية تعمل الدول العربية في إطارها - يهدد استقرار المنطقة، فنتيجة للطبيعة الخاصة بالفضاء السيبراني، من صعوبة في منع الهجمات السيبرانية بصورة كلية من الأساس نتيجة للهجمات الصفرية أو الثغرات التي يتم اكتشافها حديثًا أو الفيروسات والأسلحة السيبرانية التي يتم تطويرها، فضلًا عن صعوبة تعقب مصدر الهجمة ومعرفة الفاعل من الناحية الفنية، فإن تحقيق الأمن الوطني السيبراني بصورة كاملة أمر في غاية التعقيد.

كما أن «الردع» بطرقه التقليدية قد لا يتحقق في أفضل الأحوال في الفضاء السيبراني، ولم يثبت بعد نجاحًا فعليًّا كما في حالات الردع التقليدي، وهو ما يهدد بارتفاع حدة الصراعات السيبرانية إلى أن تصل إلى مرحلة الحرب السيبرانية الكاملة؛ لذلك كان من الضروري صياغة إستراتيجية مشتركة تسهم في تطوير القدرات السيبرانية الدفاعية للدول العربية.

ويتحقق ذلك من خلال التعاون الإستراتيجي بين دول المنطقة بمشاركة المعلومات والبيانات اللازمة لتحليل الأدلة الجنائية الرقميةDigital Evidence، التي تساعد على اكتشاف الهجمات السيبرانية فور حدوثها والعمل على تخفيف آثارها، وتتبع المعاملات

المالية المقرصنة وكذلك العملات المشفرة، التي قد تستخدم في تمويل الحركات المتمردة والإرهابية، بالإضافة إلى عمل محاكاة حرب سيبرانية بين الدول الإقليمية؛ لضمان جاهزية جميع الوحدات السيبرانية القتالية، والتعاون الفني والتقني لتطوير قدرات سيبرانية هجومية مشتركة، ولضمان الارتقاء بالمستوى المهاري والفكري للكادر البشري.

خاتمة:

إن تطور شكل الحرب عبر التاريخ من الحجارة والرماح إلى السهام والسيوف إلى المسدسات والبنادق إلى الصواريخ والقاذفات ثم إلى الدبابات والطائرات والغواصات وصولًا إلى القنابل النووية والهيدروجينية، ينذر بالقول إن من لا يدرك جيدًا تغير طبيعة وعصر وسلاح المعركة القادمة ويسارع بالحصول عليه وتطويره، سوف ينتهي به الأمر مهزومًا تابعًا لغيره ضعيفًا بين الأمم، وكلما ازدادت الدول علمًا وتقدمًا ازدادت معها القدرة التدميرية للأسلحة المستخدمة، وسلاح الحرب القادمة سوف يكون أقوى وأبشع من أشد القنابل التقليدية فتكًا؛ فالجنود المقاتلون في هذه المعركة هم من الربوتات والدرونز، والأسلحة عبارة عن شفرات وفيروسات وديدان مبرمجة، لا يتعدى حجمها بِضعة كيلوبايتات، ولكنها قادرة على إحداث تأثير يفوق في قوته الأسلحة التقليدية.

ومن هنا، يجب الاستعداد لمرحلة جديدة من الحرب البشرية، التي باتت قادمة لا محالة، وهي الحرب السيبرانية، من خلال تطوير القدرات الوطنية السيبرانية وإنشاء وحدات سيبرانية عسكرية داخل صفوف القوات المسلحة والاهتمام بتطوير ترسانة من الأسلحة السيبرانية، بالإضافة إلى صياغة إستراتيجية وطنية تعمل في إطار إستراتيجية أخرى قومية تضمن الحفاظ على الأمن الإقليمي والأمن الوطني.

قائمة المراجع

المراجع العربية:

- القرصنة الالكترونية (2021). بايدن يتعهد بعمل أمريكي ضد الهجمات الروسية. BBC. متاح عبر الرابط: https://www.bbc.com/arabic/world-57786593
- خليفة، إيهاب (2021). الحرب السيبرانية: الاستعداد لقيادة المعارك العسكرية في الميدان الخامس. دار العربي للنشر والتوزيع، القاهرة.
- لوديرميلك، ميكا (2019). الأزمة الإيرانية تنتقل إلى الفضاء السيبراني. معهد واشنطن لسياسة الشرق الأدنى، متوفر عبر الرابط: https://www.washingtoninstitute.org/ar/policy-analysis/alazmt-alayranyt-tntql-aly-alfda-alsybrany

المراجع الإنجليزية:

- Canongia, C. & Mandarino, R. (2014). Cybersecurity: The new challenge of the information society. In Crisis Management: Concepts, Methodologies, Tools and Applications, Hershey, PA: IGI Global, 60.
- Committee on National Security Systems: glossary (2015). National security agency, CNSSI No. 4009, 40, available at: https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf

news/heres-a-simple-explanation-of-how-the-massive-solarwinds-hack-happened-and-why-its-such-a-big-deal/articleshow/79945993.cms

- Lewis, J. (2006). Cybersecurity and critical infrastructure protection. Center for Strategic and International Studies, Washington, DC. Avaialbe at: http://csis.org/publication/cybersecurity-andcriticalinfrastructure-protection
- Metzger, T. & Bendiek, A. (2015) Deterrence theory in the cyber-century: Lessons from a state-of-the-art literature review. Research division EU/Europe, Working papers.
- National Initiative for Cybersecurity Careers and Studies (2021). A Glossary of Common Cybersecurity Terminology. Available at: http://niccs.us-cert.gov/glossary#letterc
- Newman, N. (2021, July 12) Russian hackers hit US and Europe. Is Asia the next target of a Massive Attack?, South China Morning Post. Available at: https:/www.scmp.com/weekasia/opinion/article/3140394/russianhackers-hit-us-and europe-asia-nexttarget-massive-attack
- NATO (2019). Cyber defence. Available at: https://www.nato.int/cps/en/natolive/75747.htm
- Craigen, D. & Diakun-Thibault, N. & Purse, R. (October 2014). Defining cybersecurity. Technology innovation management review, 15. Avaialbe at: https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf
- Cybersecurity guide for developing countries (2009). ITU. Available at: https://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf
- Eastwood, G. (2017). How smart cities can protect against IoT security threats, Network world. Available at: https://www.networkworld.com/article/3231988/internet-of-things/how-smart-cities-can-protect-againstiot-security-threats.html
- Government of Canada (2010). Canada's Cyber Security Strategy. Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/indexen.aspx
- International Telecommunication Union (2020). Global cybersecurity Index 2020, 25.
- Jibilian, I. (2021, April 15). The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal. Businessinsider India. Avaialbe at: https://www.businessinsider.in/tech/

researcherswarn-of-espionage-campaign-indiaamong-the-most-affected-nations/article32478808.ece
- Trujillo, C. (2014). The limit of Cyberspace Deterrence. The Air war college, Air university, 45.
- Wired (2014). The New eyes of surveillance: Artificial intelligence and humanizing technology. Availabe at: https://www.wired.com/insights/2014/08/the-neweyes-of-surveillance-artificial-intelligenceand-humanizing-technology/
- NATO (2016). Warsaw Summit Communiqué. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber18-Metzger, Tobias, (2015), Deterrence theory in the cyber-century, Research Division EU/Europe.
- The hindu business line (2020, Auguest 30) Cybersecurity researchers warn of espionage campaign: India among the most affected nations. Avaialbe at: https:// www.thehindubusinessline.com/info-tech/cybersecurity-

Received 06 Sep. 2021; Accepted 03 Oct. 2021; Available Online 31 Dec. 2021.

Keywords: Security Studies, Fifth domain, cyber space, national security, cyber security

الكلمات المفتاحية: دراسات أمنية، الميدان الخامس، الفضاء السيبراني، الأمن الوطني، الأمن السيبراني.

Production and hosting by NAUSS

* Corresponding Author: Ehab Khalifa
Email: ehabakhalifa@gmail.com
doi: 10.26735/ACPS7277