

Distr.: General  
15 July 2021  
Arabic  
Original: English



الدورة السادسة والسبعون

البند 74 من جدول الأعمال المؤقت\*

حق الشعوب في تقرير المصير

## استخدام المرتزقة وسيلة لانتهاك حقوق الإنسان وإعاقة ممارسة حق الشعوب في تقرير مصيرها

مذكرة من الأمين العام

يشرف الأمين العام أن يحيل إلى الجمعية العامة تقرير الفريق العامل المعنى بمسألة استخدام المرتزقة وسيلة لانتهاك حقوق الإنسان وإعاقة ممارسة حق الشعوب في تقرير مصيرها، وفقاً لقرار الجمعية العامة 171/75 وقرار مجلس حقوق الإنسان 9/42.



الرجاء إعادة استعمال الورق

\* A/76/150

130821 050821 21-09837 (A)



## تقرير الفريق العامل المعنى بمسألة استخدام المرتزقة وسيلة لانتهاك حقوق الإنسان وإعاقة ممارسة حق الشعوب في تقرير مصيرها

آثار المرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة والشركات العسكرية والأمنية الخاصة التي تشارك في أنشطة إلكترونية على حقوق الإنسان

### موجز

في هذا التقرير، يتناول الفريق العامل المعنى بمسألة استخدام المرتزقة وسيلة لانتهاك حقوق الإنسان وإعاقة ممارسة حق الشعوب في تقرير مصيرها مسألة توفير المرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة والشركات العسكرية والأمنية الخاصة للمنتجات والخدمات العسكرية والأمنية في الفضاء الإلكتروني وآثارها على حقوق الإنسان.

وهناك طائفة واسعة من الخدمات العسكرية والأمنية المقدمة في الفضاء الإلكتروني، بما في ذلك جمع البيانات والاستخبارات والتجسس. ويمكن أن تستعين الدول والجهات من غير الدول بجهات فاعلة خاصة في إطار علاقات غير مباشرة لإجراء عمليات هجومية أو دفاعية، وحماية الشبكات والبنى التحتية الخاصة بها، ولتنفيذ عمليات سيبرانية لإضعاف القدرات والإمكانات العسكرية للقوات المسلحة المعادية، أو لتقويض سلامة إقليم دول أخرى. ويمكن للأفراد الذين ينفذون هجمات إلكترونية أن يتسببوا في أضرار عن بعد، عبر ولايات قضائية مختلفة. ولذا، يمكن أن يُنظر إلى هؤلاء الأفراد على أنهم يقومون بنشاط ذي صلة بالمرتزقة، أو حتى بنشاط من أنشطة المرتزقة إذا استوفيت كل المعايير التي تجعل هذا الوصف منطبقاً عليه.

وتهدف هذه الدراسة المواضيعية إلى استكشاف مظاهر وأنشطة هذه الجهات الفاعلة التي تستفيد من تطوير القدرات السيبرانية وصيانتها وتشغيلها، التي يمكن استخدامها في الأعمال العدائية، وفي حالات النزاع وفي غير حالات النزاع. وتقيّم الآثار التي قد تترتب على ذلك في مجال حقوق الإنسان، بما في ذلك حق الشعوب في تقرير مصيرها، كما تتناول مسألة تنظيم توفير المنتجات والخدمات العسكرية والأمنية في الفضاء الإلكتروني.

وخلال فترة إعداد هذا التقرير، تألف الفريق العامل من يلينا أباراك (رئيسة)، ويليان بوبيا، ورافيندران دانيال، وكريس كواجا، وسورشا ماكليود.

## المحتويات

## الصفحة

4	أولا - المقدمة والسياق .....
5	ثانيا - اعتبارات التعريف .....
6	ثالثا - الخدمات العسكرية والأمنية في الفضاء الإلكتروني: الأنشطة وفئات الجهات الفاعلة والعلاقات بين الجهات من الدول ومن غير الدول .....
8	ألف - فئات الجهات الفاعلة ذات الصلة في الفضاء الإلكتروني .....
11	باء - العلاقات بين الجهات من الدول ومن غير الدول .....
13	رابعاً - تنظيم دور المرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة والشركات العسكرية والأمنية الخاصة ومشاركتها في توفير الخدمات الإلكترونية .....
13	ألف - ميثاق الأمم المتحدة .....
15	باء - القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني .....
16	جيم - القانون الجنائي الدولي .....
17	دال - القانون غير الملزم والمبادرات الجارية .....
18	خامساً - الآثار في مجال حقوق الإنسان .....
21	سادساً - استنتاجات وتوصيات .....

## أولا - المقدمة والسياق

- 1 - هذا التقرير مقدم إلى الجمعية العامة من الفريق العامل المعني بمسألة استخدام المرتزقة وسيلة لانتهاك حقوق الإنسان وإعاقة ممارسة حق الشعوب في تقرير مصيرها، وفقاً لقرار الجمعية العامة 171/75 وقرار مجلس حقوق الإنسان 9/42.
- 2 - وسعياً إلى الاضطلاع بهذه الولاية، يرصد الفريق العامل المرتزقة والأنشطة المتصلة بالمرتزقة بجميع أشكالها ومظاهرها، وكذلك الشركات العسكرية والأمنية الخاصة في مختلف أنحاء العالم. وإضافة إلى ذلك، يدرس الفريق العامل أنشطتها وتأثيرها على حقوق الإنسان، لا سيما الحق في تقرير المصير.
- 3 - ويعتمد التقرير على البحوث النظرية المستفيضة وعلى المساهمات الواردة من الجهات المعنية بناء على دعوة وجهها الفريق العامل في كانون الثاني/يناير 2021 لتقديم مساهمات<sup>(1)</sup>. وفي 7 كانون الأول/ديسمبر 2020، عقد الفريق العامل مشاوراً للخبراء على الإنترنت بشأن المرتزقة والجهات الفاعلة ذات الصلة في سياق أمن الفضاء الإلكتروني والتكنولوجيات الجديدة بغية إثراء التقرير بنتائجها. ويشكر الفريق العامل كل من ساهموا في إعداد التقرير بتقديم معلومات والمشاركة في مشاورات الخبراء.
- 4 - وركزت المناقشات بشأن أنشطة المرتزقة على مر السنين على أساليب الحرب التقليدية التي يشارك فيها المرتزقة بالنيابة عن الدول أو عن عملاء آخرين. وفي الآونة الأخيرة، بدأت المرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة والشركات العسكرية والأمنية الخاصة تقوم بأنشطة في الفضاء الإلكتروني. وأشار الفريق العامل، في تقريره عن الأشكال والاتجاهات والمظاهر الآخذة في التطور للمرتزقة والأنشطة المتصلة بهم (انظر الوثيقة A/75/259)، إلى ما يسمى "مرتزقة الفضاء الإلكتروني" باعتبارهم فئة من الجهات الفاعلة التي يمكنها أن تولد أنشطة متصلة بالمرتزقة. وإضافة إلى ذلك، تثار بانتظام مسألة استخدام التكنولوجيا ونقل المعارف في التقارير السنوية للفريق العامل فيما يتعلق بمختلف المواضيع<sup>(2)</sup>. ويتناول هذا التقرير مسألة توفير المرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة والشركات العسكرية والأمنية الخاصة للمنتجات والخدمات العسكرية والأمنية في الفضاء الإلكتروني، وأثارها على حقوق الإنسان.
- 5 - وأشار الفريق العامل في تحليلاته السابقة إلى مجموعة المرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة التي لا تزال تؤثر على مسار النزاعات المسلحة المعاصرة، وترتكب انتهاكات لحقوق الإنسان، وتقوض الحق في تقرير المصير، بوسائل منها الأنشطة الإلكترونية. واليوم، يمثل الفضاء الإلكتروني ساحة جيوسياسية رئيسية لكل من الجهات من الدول ومن غير الدول، حيث تقوم مجموعة متنوعة من الكيانات الخاصة بتعبئة وتسخير قدرات إلكترونية دفاعية وهجومية على حد سواء سعياً إلى تنفيذ خطط أو تحقيق مصالح بوسائل غير مباشرة، مع ما يترتب على ذلك من عواقب مدمرة على التمتع بحقوق الإنسان وعلى حق الشعوب في تقرير مصيرها.
- 6 - وعلى وجه الخصوص، أشار الفريق العامل في السابق إلى تزايد الطابع غير المتناظر للنزاعات المسلحة الحديثة، وإلى ازدياد مشاركة الجهات الفاعلة الخاصة (A/75/259). ولئن كانت الحرب الحركية

(1) انظر الرابط التالي: [www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Report-Cyber-Mercenaries-2021.aspx](http://www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Report-Cyber-Mercenaries-2021.aspx).

(2) انظر الوثائق A/75/259، الفقرة 50؛ و A/HRC/45/9، الفقرة 39 وما يليها؛ و A/HRC/42/42.

التقليدية لا تزال تؤدي دورا رئيسيا في النزاع المعاصر، يسود استخدام الهجمات الإلكترونية وغيرها من أنشطة الفضاء الإلكتروني بشكل متزايد مع تطوير تكنولوجيات جديدة واستمرار تطورها، حتى خارج النزاعات المسلحة التقليدية. وكنتيجة طبيعية لهذه التطورات، تكيف المرتزقة المعاصرون وغيرهم من الجهات الفاعلة وأصبحوا نشطين في الفضاء الإلكتروني، وفي بعض الحالات، أصبحوا عنصرا ضروريا في العمليات السيبرانية.

## ثانيا - اعتبارات التعريف

7 - يرد تعريف مصطلح "المرتزقة" في المادة 47 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام 1949، والاتفاقية الدولية لمناهضة تجنيد المرتزقة واستخدامهم وتمويلهم وتدريبهم، واتفاقية منظمة الوحدة الأفريقية للقضاء على أعمال المرتزقة في أفريقيا. بيد أن تعريف الجندي "المرتزق" في القانون الدولي كان موضع كثير من التحليل والتفكير حول طابعه التقييدي المفرط. ويسلم الفريق العامل بأن نطاق التعريف ينطوي على إشكاليات وأنه يصعب استيفاء المعايير، لا سيما فيما يتعلق بالأشكال المعاصرة للأنشطة المتصلة بالمرتزقة، بما في ذلك عندما تقوم بهذه الأنشطة جهات من غير الدول في الفضاء الإلكتروني.

8 - وإضافة إلى ذلك، في غياب تعريف قانوني متفق عليه دوليا، سبق للفريق العامل أن عرّف عبارة "الشركات العسكرية والأمنية الخاصة" بأنها تعني شركات ذات كيان قانوني تقدم، بمقابل مادي، خدمات عسكرية و/أو أمنية بواسطة أشخاص طبيعيين و/أو كيانات قانونية<sup>(3)</sup>. وقد تعمل في حالات النزاع ووقت السلم على حد سواء، وهي من كبريات الجهات المقدمة للمنتجات والخدمات العسكرية والأمنية في المجال الإلكتروني.

9 - ولا يتضمن أي من التعاريف المذكورة أعلاه إشارة صريحة إلى الأنشطة أو الجهات الفاعلة في الفضاء الإلكتروني، ولكن من الواضح أن بعض الإجراءات في المجال الإلكتروني قد ترقى إلى مستوى الارتزاق أو تُعتبر أنشطة متصلة بالمرتزقة، وتؤثر أيضا على حقوق الإنسان في النزاعات المسلحة وفي أوقات السلم على حد سواء. ويمكن أن تشمل هذه الإجراءات العمليات السيبرانية الخبيثة التي يقوم بها وسطاء سيبرانيون بغض النظر عن جنسيتهم أو مكان عملياتهم، أو سواء كانوا يعملون خارج شبكة الإنترنت أو عبرها، أو يسيبون ضررا بشكل مباشر أو غير مباشر<sup>(4)</sup>. ويقصد من العمليات السيبرانية الخبيثة استخدام إجراءات وعمليات متعمدة لتغيير النظم أو الشبكات الحاسوبية أو تعطيلها أو خداعها أو إضعافها أو تدميرها، أو تقويض سرية النظم أو الشبكات الحاسوبية للأفراد والمجتمعات وسلامتها وتوافرها بطريقة أخرى<sup>(5)</sup>. ولا يشمل ذلك التكنولوجيات الناشئة، مثل تكنولوجيا المركبات الموجهة عن بعد، التي لها آثار حركية خارج الشبكات الحاسوبية.

10 - غير أن الفريق العامل يود أن يؤكد على أنه لا ينبغي أن يُعتبر أن الخدمات العسكرية والأمنية المقدمة في الفضاء الإلكتروني تدل على عمليات الجهات الفاعلة المتصلة بالمرتزقة بشكل عام، بل يتعين

(3) للاطلاع على التعريف الكامل، انظر الوثيقة A/HRC/15/25، المرفق، المادة 2.

(4) Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018), p. 31

(5) Herbert S. Lin, "Offensive cyber operations and the use of force", *Journal of National Security Law and Policy*, vol. 4, No. 1 (13 August 2010), pp. 4–63; and ISO/IEC 27000:2009.

تقييم كل حالة محتملة ناشئة من بين هذه الفئات في ضوء سياقها وظروفها المعينة (انظر الوثيقة A/75/259، الفقرة 54).

11 - وفي عام 2020، اعترف الفريق العامل بأن الحرب السيبرانية أسلوب من أساليب الحرب التي لا تقتصر قدراتها على التسلل أو التعطيل أو إلحاق الضرر بالأهداف العسكرية أو الأعيان المدنية أو حتى تدميرها فحسب، بل إنها تسبب أيضاً أضراراً بشرية فادحة. وخلصت اللجنة الدولية للصليب الأحمر إلى أنه يجب أن تمتثل للقانون الدولي الإنساني<sup>(6)</sup>. وتزداد أهمية ذلك نظراً لاعتماد القدرات الاستراتيجية بشكل متزايد على البنى التحتية والتكنولوجيا (انظر الوثيقة A/75/259، الفقرة 42).

12 - ومما دفع الفريق العامل إلى تسليط الضوء على هذه الظاهرة تحول النزاعات المعاصرة وسرعة تطور الأشكال الجديدة من الحروب إلى جانب انعدام التنظيم والرصد والرقابة، فضلاً عن صعوبات التحقيق في الجرائم التي ترتكب عبر الولايات القضائية، من بين أمور أخرى. كما أن عدم المساواة في حصول بعض البلدان المتقدمة النمو والجهات الفاعلة النثرية على التكنولوجيات وما يتصل بها من معرفة من جانب يثير قلق الفريق العامل.

13 - ويدرك الفريق العامل أن السياقات التي يعمل فيها المرتزقة تؤثر تأثيراً متبايناً وغير متناسب على النساء والأطفال وغيرهم من الفئات (انظر الوثيقة A/75/259، الفقرة 5). ويشير الفريق العامل أيضاً إلى الصعوبات الناشئة عن عدم وجود تعريف متفق عليه دولياً لما يشكل هجوماً إلكترونياً أو أعمالاً عدائية إلكترونية في إطار القانون الدولي الإنساني، ولذلك يصعب حالياً من الناحية المفاهيمية حصر الأعمال العدائية الإلكترونية في إطار القانون الدولي الإنساني وتحديد عدم الامتثال والانتهاكات.

14 - ومن العناصر البالغة الأهمية في النقاش الدائر حول معرفة متى وأين وكيف يمكن تنظيم هذه الأنشطة السيبرانية، ودور الجهات الفاعلة من غير الدول في الأنشطة السيبرانية والحرب السيبرانية، لا سيما المرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة والشركات العسكرية والأمنية الخاصة، وكذلك الكيانات الخاصة والتجارية الأخرى. ولذلك يسعى الفريق العامل في هذا التقرير إلى تناول طائفة من الخدمات العسكرية والأمنية المقدمة في الفضاء الإلكتروني التي يمكن أن تولد أنشطة متصلة بالمرتزقة، بغية إثارة مناقشة بشأن كيفية وضع إطار لها ومعالجتها بوجه أفضل (انظر الوثيقة A/75/259، الفقرة 52). وإلى جانب الضوابط التنظيمية، يجب إقامة تعاون فعال على الصعيدين الوطني والدولي بين الجهات الفاعلة ذات الصلة تصدياً لهذه الظاهرة.

### ثالثاً - الخدمات العسكرية والأمنية في الفضاء الإلكتروني: الأنشطة وفئات الجهات الفاعلة والعلاقات بين الجهات من الدول ومن غير الدول

15 - تشمل الخدمات العسكرية والأمنية طائفة من الخدمات منها جمع البيانات والتجسس. ويمكن أن تستعين الدول والجهات من غير الدول بجهات فاعلة خاصة في إطار علاقات غير مباشرة لإجراء عمليات هجومية أو دفاعية، وحماية الشبكات والبنى التحتية الخاصة بها، وكذلك تنفيذ عمليات سيبرانية

(6) اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة"، ورقة موقف، تشرين الثاني/نوفمبر 2019.

لإضعاف القدرات والإمكانات العسكرية للقوات المسلحة المعادية، أو لتقويض سلامة إقليم دولة أخرى. وهذه الجهات الفاعلة، باستخدامها لقوة نيرانها الإلكترونية الهجومية أو الدفاعية، ترتبط بمحاولات أو أعمال ترمي إلى تحديد المنشآت العسكرية أو المدنية البالغة الأهمية أو الاعتداء عليها أو تشويشها، بهدف تدميرها.

16 - وكما ذكر أعلاه، من المهم الإشارة إلى أن الخدمات السيبرانية تقدّم إلى الدول خارج سياق النزاع المسلح، لأغراض لا تقتصر على جمع المعلومات الاستخبارية ومراقبتها، ولكن منها أيضا إنفاذ القانون المحلي وحفظ الأمن<sup>(7)</sup>. وإضافة إلى ذلك، تشمل الخدمات السيبرانية توفير خدمات الدعم للدول فيما يتعلق بالقدرات السيبرانية القائمة وتوفير المنتجات السيبرانية التي يمكن أن تستخدمها الدول على حد سواء. ومن المهم الإشارة إلى أنه يجري توفير مجموعة واسعة من المنتجات والخدمات وهي متاحة للشراء في السوق المفتوحة، ويجب مراعاة ذلك عند النظر في تنظيم الخدمات السيبرانية.

17 - ومن أنواع الأنشطة السيبرانية وأساليب العمل المتعددة التي يتم الاضطلاع بها حاليا، في جملة أمور، التخريب بواسطة البرمجيات الخبيثة وفيروسات الفدية، والتجسس، والتخريب الذي ينطوي على توفير المعلومات الخاطئة والمعلومات المضللة. ومن الناحية العملية، يمكن أن تتخذ هذه الأنشطة شكل إغلاق أو إتلاف أجزاء رئيسية من البنية التحتية، بما في ذلك إمدادات الكهرباء والمياه، والمستشفيات، وخدمات المراقبة، ومرافق الاتصالات، أو يمكن أيضا أن تسهل استهداف أو تعطيل الدفاع العسكري وغيره من النظم.

18 - وتوفر شركات الأمن السيبراني، في عملها لصالح الشركات الخاصة والدول، خدمات دفاع ضد الهجمات الإلكترونية والحرب الإلكترونية. وتشمل هذه العمليات الدفاعية البحتة جدران الوقاية وتصحيح البرامج وبرمجيات مكافحة الفيروسات، في حين توجد خطوات أكثر نشاطا ولكنها لا تزال دفاعية منها إنشاء مصاديد لقرصنة الإنترنت، وفخاخ، والإنارة لتحذير المهاجمين وإيقاعهم<sup>(8)</sup>. وسواء كانت هذه العمليات الدفاعية سلبية أو فعالة، فإنها تندرج ضمن المبادئ التوجيهية القانونية القائمة لعمليات الأمن السيبراني.

19 - بيد أن شركات الأمن السيبراني، سواء منها الخاصة والحكومية، وكذلك المشغلين الخارجيين عن القانون، لها أيضا قدرات هجومية، وذلك مجال يثير قلقا خاصا لدى الفريق العامل. ويمكن استخدام القدرات الهجومية لشركات الأمن السيبراني ضد دول متقدمة النمو، كما هو الحال في الهجمات على البنية التحتية للانتخابات، التي يفترض أن تنفذها جهات فاعلة ترعاها الدولة أو وكلاء يعملون لصالح الدول. ومن الأنشطة السيبرانية الخبيثة أيضا استهداف الأصول الافتراضية ومقدمي خدمات الأصول الافتراضية، والهجمات على شركات الدفاع، بما في ذلك الهجمات الرامية إلى الوصول إلى التكنولوجيا العسكرية بصورة غير مشروعة (انظر الوثيقة S/2021/211، المرفق، الفقرتان 125 و 126). ولا يوجد نمط موحد واضح وجلي تتسم به الجهات من الدول ومن غير الدول التي تشتري هذه التكنولوجيات. فالدول الديمقراطية وغير الديمقراطية على حد سواء تقتني تكنولوجيات هجومية من مقدمي خدمات خارجيين، كما تفعل الدول التي لها قدرات سيبرانية داخلية والدول التي ليس لديها مثل هذه الموارد.

20 - وتتمو سوق القدرات السيبرانية الهجومية نموا سريعا، ولا تكاد تخضع لتنظيم يذكر، وتوفر فرصة لتحقيق أرباح كبيرة. ونتيجة لذلك، تقوم العديد من الشركات العسكرية والأمنية الخاصة التقليدية بتطوير

(7) انظر المساهمة التي قدمتها مؤسسة تكنولوجيا المعلومات والاتصالات من أجل السلام.

(8) مساهمة قُدمت تحت الختم.

أقسام الأمن السيبراني<sup>(9)</sup>. وأيا كان مصدر مقدمي خدمات الأمن السيبراني، مثل الشركات العسكرية والأمنية الخاصة الأكثر تقليدية، يعملون جنباً إلى جانب مع الحكومات الوطنية ويصبحون امتداداً لسلطة الدولة، وبالتالي يمكن اعتبارهم وكلاء يشبهون المرتزقة.

21 - ويمكن أيضاً أن تنطبق الفروق بين الخدمات الهجومية والدفاعية وكذلك الفروق بين الشفافية والغموض بشأن الوضع القانوني على الخدمات العسكرية والأمنية المقدمة في الفضاء الإلكتروني. ويمكن أيضاً أن تتعاون الدول والجهات الفاعلة من غير الدول مع الجهات الفاعلة الخاصة ليس بغرض حماية الشبكات والبنى التحتية الخاصة بها فحسب، ولكن أيضاً لتنفيذ عمليات سيبرانية رامية إلى إضعاف القدرات والإمكانات العسكرية للقوات المسلحة المعادية، أو لتقويض سلامة إقليم دولة أخرى. ووجود المرتزقة في الفضاء الإلكتروني حيث يشاركون الآن في إنتاج الأسلحة السيبرانية الهجومية وبيعها يؤكد قدرتهم على التكيف<sup>(10)</sup>. ولذا، يمكن أن يُنظر إلى الأفراد الذين يقومون بهجمات إلكترونية على أنهم يقومون بنشاط ذي صلة بالمرتزقة، أو حتى بنشاط من أنشطة المرتزقة إذا استوفيت كل المعايير التي تجعل هذا الوصف منطبقاً عليه (انظر الوثيقة A/75/259، الفقرة 71).

## ألف - فئات الجهات الفاعلة ذات الصلة في الفضاء الإلكتروني

### الوحدات أو القيادات السيبرانية المدمجة ضمن القوات المسلحة الرسمية

22 - في السنوات الأخيرة، حفزت استراتيجيات التأثير السيبراني المنافسة على الخبرة السيبرانية التي أظهرت الآثار المدمرة على العلاقات الجيوسياسية الحديثة<sup>(11)</sup>. وتشارك بعض الدول فيما وصف بأنه "معركة معلوماتية في الفضاء الإلكتروني"<sup>(12)</sup> وتدمج عمليات استراتيجية النفوذ العسكرية في قدراتها العسكرية. وأدى التطور السريع للتكنولوجيات الرقمية إلى تحويل الحرب بشكل عميق ودفع إلى الاستثمار في تطوير وحدات إلكترونية أو قيادة إلكترونية مدمجة في القوات المسلحة الرسمية. وعلاوة على ذلك، فإن أشكال الحرب التقليدية بين قوتين مسلحتين تصاحبها الآن حرب إلكترونية، حيث تعمل وحدات سيبرانية على طول الخطوط الرفيعة الفاصلة بين العمليات الدفاعية والهجومية<sup>(13)</sup>. ويمكن أن تُنفذ العمليات السيبرانية الهجومية وحدها أو بالاقتران مع العمليات العسكرية التقليدية. غير أن أكثر السيناريوهات إثارة للقلق هي تلك المرتبطة بحالة "العمليات الهجينة" حيث ترد الدولة من خلال عملياتها العسكرية السيبرانية في سياق لا يعتبر أنه قد وصل إلى عتبة النزاع المسلح بمقتضى قواعد القانون الدولي الإنساني. وتكون المعركة

(9) W. J. Hennigan, "Defense contractors see opportunity in cybersecurity sector", *Los Angeles Times*, 21 January 2020. متاح على الرابط التالي: [www.latimes.com/business/la-fi-0122-cyber-defense-20150122-story.html](http://www.latimes.com/business/la-fi-0122-cyber-defense-20150122-story.html).

(10) Tom Burt, "Cyber mercenaries don't deserve immunity", Microsoft website, 21 December 2020. متاح على الرابط التالي: <https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/>.

(11) انظر الرابط التالي: <https://spire.sciencespo.fr/hdl/2441/1uu1c1r2ua9f0o7n0co15a8trv/resources/2021-03-derochegonde-tenenbaum-cyberinfluence-focus-strategique.pdf>, pp. 9-10.

(12) انظر الرابط التالي: <https://spire.sciencespo.fr/hdl/2441/1uu1c1r2ua9f0o7n0co15a8trv/resources/2021-03-derochegonde-tenenbaum-cyberinfluence-focus-strategique.pdf>, pp. 7-8.

(13) Neri Zilber, "The rise of the cyber-mercenaries: what happens when private firms have cyberweapons as powerful as those owned by governments?", *Foreign Policy* (FP), 31 August 2018. متاح على الرابط التالي: <https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/>.



المعلوماتية في الفضاء الإلكتروني أكثر تعقيدا عندما تستعين القوات المسلحة الرسمية في بعض أنشطتها السيبرانية بطرف ثالث.

### الجهات الفاعلة خارج القوات المسلحة الرسمية

23 - تؤدي الكيانات من غير الدول غير المندمجة في القوات المسلحة دورا مهما جدا وكبيراً على نحو متزايد في توفير الخدمات السيبرانية للدول ونيابة عنها. ويستشري التهديد المتغير لخصخصة هجمات الأمن السيبراني عن طريق جيل جديد من الشركات الخاصة يشار إليها باسم "مرتزقة الإنترنت"<sup>(14)</sup>، وهناك خط يزداد انطاماسا يفصل بين المجالين الخاص والوطني<sup>(15)</sup>.

### الكيانات التجارية

24 - بخلاف الشركات العسكرية والأمنية الخاصة التقليدية التي قامت عادة بخصخصة الوظائف والقدرات التي كانت في السابق تستأثر بها الدولة، ظهر مقدمو خدمات الأمن السيبراني لأول مرة وازدهروا في القطاع الخاص. ولئن اكتسبت الجيوش العالمية الأكثر تقدما خبرات وقدرات داخلية في مجال الأمن السيبراني، فحتى هذه العمليات العسكرية المتطورة تعتمد اعتمادا كبيرا على خبرة القطاع الخاص في مجال الأمن السيبراني<sup>(16)</sup>. ومن الشركات الخاصة للأمن السيبراني الجهات الفاعلة الهادفة للربح الموجودة منذ عهد طويل والشركات الناشئة الحيوية التي فازت بحصص في سوق سريعة التوسع.

25 - ويمكن تقسيم شركات البرمجيات والتكنولوجيا الخاصة التي تقع ضمن نطاق التحليل إلى فئتين. وتتألف الفئة الفرعية الأولى من منصات تكنولوجيا كبيرة تعمل بالتواطؤ مع الجهات الحكومية من أجل تمكين الحكومات من الاطلاع على المعلومات وتشغيل برامج المراقبة<sup>(17)</sup>. أما الفئة الفرعية الثانية فتتكون من شركات أصغر بكثير من حيث الحجم ومستوى الإيرادات، ولكن لديها قدرات معينة لصناعة المنتجات التي يمكن استخدامها للقيام بأنشطة خبيثة. ويشهد قطاع شركات الأمن السيبراني الخاصة نموا وتطورا سريعين. وإضافة إلى ذلك، انتقلت عدة شركات عسكرية وأمنية خاصة إلى قطاع الأمن السيبراني، غالبا باقتناء شركات تكنولوجيا متخصصة وتحويلها إلى شركات داخلية.

26 - وقامت شركات عاملة في قطاع الدفاع التي كانت تقليديا تنتج الأسلحة والمعدات العسكرية بتوسيع نطاق أنشطتها لتشمل القطاع الرقمي. وطور هؤلاء المقاتلون إلى حد كبير حلولاً وخدمات داخلية للأمن السيبراني، رغم أن بعضهم استعان أيضا بشركات تجارية للأمن السيبراني باعتبارها شركات فرعية لتعزيز قدراتهم. والرسائل الموجهة من شركات الأسلحة إلى الجمهور تطمس عمدا الخطوط الفاصلة بين الإجراءات والخدمات التي لا تستهدف إلا مجرد الدفاع عن قدرة الفضاء الإلكتروني على الصمود، وبين التكنولوجيات التخريبية التي من شأنها أن تتيح للعملاء القيام بعمليات هجومية وأنشطة خبيثة محتملة.

(14) انظر المساهمة التي قدمتها مؤسسة منظمة الوصول الآن، الصفحة 1.

(15) انظر المساهمة التي قدمها أوري سويد ودانيال بورلاند، الصفحة 15.

(16) انظر الرابط التالي: [www.cmi.no/publications/file/6637-russian-use-of-private-military-and-security.pdf](http://www.cmi.no/publications/file/6637-russian-use-of-private-military-and-security.pdf).

(17) انظر الرابط التالي: <https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/>.

## الجماعات التي تشكل تهديدا متواصلا متطورا

27 - إن أعضاء الجماعات التي تشكل تهديدا متواصلا متطورا جهات فاعلة مارقة/إجرامية تشارك في اختراق مستمر لأنظمة الأمن السيبراني للدول والجهات الفاعلة في القطاعين العام والخاص. فهي متطورة من الناحية التكنولوجية، وتمتلك موارد مالية وتقنية هامة، ولها أهداف استراتيجية طويلة الأجل، وكثيرا ما تدعمها الحكومات الوطنية بطريقة أو بأخرى<sup>(18)</sup>. ولديها القدرة الداخلية على تطوير قدرات هجومية ويمكنها القيام بعمليات سيبرانية واسعة النطاق. وتطلق الشَّعب السيبرانية في الجيوش الوطنية أيضا تهديدات متواصلة متطورة. كما أن خدمة "قراصنة للإيجار" قد توضع على المحك بشكل مستمر نظم الدفاع الإلكترونية للشركات الخاصة والحكومات. والجماعات التي تشكل تهديدا متواصلا متطورا مرتبطة، بحكم طبيعتها، بهدف أطول أجلا من الهدف المتمثل في تحقيق أرباح سريعة من خلال استخدام فيروس الفدية.

## ميليشيات الفضاء الإلكتروني

28 - هناك فئة أخرى تتألف مما يسمى ميليشيات الفضاء الإلكتروني، وتضم مجموعة متنوعة من المنظمات يتعهد بها متطوعون. وبهذه الصفة، قد تتجاوز هذه الميليشيات نطاق المرتزقة أو الجهات الفاعلة ذات الصلة بالمرتزقة. وهي تختلف عن الجماعات التي تشكل تهديدا متواصلا متطورا حيث إنها ليست منظمة أو ممولة بشكل جيد وليس لها أهداف استراتيجية طويلة الأجل. وهناك نموذج افتراضي للميليشيات المهاجمة في الفضاء الإلكتروني التي تعتمد على المتطوعين يميز بين المنتدى والخلية والتسلسل الهرمي. فالمنتدى هيكل مخصص لميليشيات الفضاء الإلكتروني منظم حول منصة اتصالات مركزية، حيث يتبادل الأعضاء المعلومات والأدوات اللازمة لتنفيذ هجمات إلكترونية ضد هدفهم المختار. ويتشكل نموذج الخلية في خلايا قراصنة الإنترنت، التي تشغل بالقرصنة لدوافع سياسية خلال فترات طويلة من الزمن. أما التسلسل الهرمي فيعكس النموذج الهرمي التقليدي، الذي يمكن مصادفته في المنظمات التطوعية التي ترعاها الحكومة، ولدى جهات فاعلة متماسكة ذاتية التنظيم غير تابعة لدول. وتشمل فئة ميليشيات الفضاء الإلكتروني أيضا مجموعات منظمة من أخصائيي الفضاء الإلكتروني الذين يتطوعون لصَدِّ الهجمات الإلكترونية<sup>(19)</sup>.

## الأفراد

29 - غالبا ما يعمل خبراء الفضاء الإلكتروني الذين يمتلكون خبرة تقنية في تكنولوجيا المعلومات خارج أي بنية تنظيمية ويقومون بإجراء أبحاث مستقلة لاكتشاف مواطن الضعف أو الأخطاء البرمجية<sup>(20)</sup>. ويعرف هؤلاء الأفراد بأنهم باحثون أمنيون وقد يبيعون معلومات مرتبطة بمواطن الضعف المذكورة إلى الخصوم<sup>(21)</sup>.

(18) انظر الرابط التالي: <https://targetedthreats.net/media/1-ExecutiveSummary.pdf>.

(19) انظر Rain Ottis, "Proactive defence tactics against on-line cyber militia", in *Proceedings of the 9th European Conference on Information Warfare and Security*, Thessaloniki, Greece, 01–02 July (Reading, United Kingdom, Academic Publishing, 2010), pp. 233–237.

(20) Steve Ranger, "Meet the hackers who earn millions for saving the web, one bug at a time", ZD Net, 16 November 2020. Available at [www.zdnet.com/article/meet-the-hackers-who-earn-millions-for-saving-the-web-how-bug-bounties-are-changing-cybersecu](http://www.zdnet.com/article/meet-the-hackers-who-earn-millions-for-saving-the-web-how-bug-bounties-are-changing-cybersecu).

(21) انظر المساهمة التي قدمتها الرابطة النسائية الدولية للسلم والحرية.

وتبعا للسياق، غالبا ما يتلقون أجورا عن هذا العمل من خلال مدفوعات تعرف باسم "مكافآت اكتشاف الأخطاء البرمجية". وهم يتصلون بالعملاء المحتملين عبر بوابات إلكترونية.

### مجرمو الفضاء الإلكتروني

30 - عصابات الابتزاز الإجرامي جهات إجرامية مارقة لا تهدف بالضرورة إلى تعطيل الاقتصاد أو القيام بالتخريب السياسي، ولكن إلى استغلال حيابة بيانات الشركات كوسيلة للابتزاز. وهذه العصابات أفراد أو جماعات تعمل لمصلحتها الخاصة باستهداف الخدمات والمنتجات والبنية التحتية التي يوفرها القطاع العام والخاص، والتي تعتمد عليها مجتمعات وفئات سكانية بأسرها. فهم ينتزعون الفدية، ولرد الجهات المستهدفة على طلب الفدية آثار اقتصادية وسياسية تتجاوز الفعل الفردي نفسه، فيما يتعلق باحتمال امتداد هذه الأنواع من الهجمات واستمرارها. فعلى سبيل المثال، يستمر التعطيل لحين دفع فدية.

### باء - العلاقات بين الجهات من الدول ومن غير الدول

31 - يمكن أن يتخذ تعامل الدول مع هذه الجهات الفاعلة في الفضاء الإلكتروني أشكالا مختلفة. ففي حالة التقويض، تمارس الدولة رقابة واضحة على تصرفات الوكلاء من خلال فرز الجهات الفاعلة واختيارها، وفرض جزاءات عقابية، وإجراء تقييم واضح للآثار المحتملة<sup>(22)</sup>. وفي هذه الحالة، تُسند مسؤوليات واضحة إلى وكلاء عبر قنوات القوانين والسياسات المحلية، مثل القيام بضربات واقية من تهديدات الفضاء الإلكتروني المتصورة<sup>(23)</sup> على البنية التحتية الحيوية<sup>(24)</sup>. وفي حالة التنسيق، تقدم الدولة دعما غير فاعل إلى الوكلاء ولكنها لا تضع آليات واضحة لمراقبة عملياتهم<sup>(25)</sup>. ويتحقق ذلك عموما من خلال أطر سياساتية غير محدّدة بدقة أو غير موجودة، والتعاون المخصص عن طريق "علاقات شبكية"<sup>(26)</sup>. وحسب نموذج الجزء، لا تعترف الدولة بالإجراءات التي تتخذها الجهات الفاعلة من القطاع الخاص التي تعمل انطلاقا من إقليمها<sup>(27)</sup>.

32 - ومن خلال عملية خصخصة بعض العمليات الإعلامية واستراتيجيات النفوذ العسكرية، تسند الدولة المهام التي لم تعد لديها القدرة على توفيرها أو الرغبة في ذلك إلى جهات فاعلة من القطاع الخاص. وينفذ

(22) Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018), p. 29

(23) Amanda N. Craig, Scott J. Shackelford and Janine S. Hiller, "Proactive cybersecurity: a comparative industry and regulatory analysis", *American Business Law Journal*, vol. 52, no. 4 (winter 2015)

(24) Ellyne Phneah, "S'pore beefs up cybersecurity law to allow preemptive measures", ZDNet, 14 January 2013، متاح على الرابط التالي: [www.zdnet.com.sg/spore-beefs-up-cybersecurity-law-to-allow-preemptive-measures-7000009757/](http://www.zdnet.com.sg/spore-beefs-up-cybersecurity-law-to-allow-preemptive-measures-7000009757/)

(25) Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018)

(26) Arindrajit Basu and Elonnai Hickok, "Conceptualizing an international framework for active private cyber defense"، متاح على الرابط التالي: [https://4bac176f-2e16-421b-823f-0ab6d7712f85.filesusr.com/ugd/066049\\_e1a28ac2850d49fbb6f52eeb9fc79ae7.pdf](https://4bac176f-2e16-421b-823f-0ab6d7712f85.filesusr.com/ugd/066049_e1a28ac2850d49fbb6f52eeb9fc79ae7.pdf)

(27) Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018)

العديد من مقدمي الخدمات مهاماً قد تكون قوات الأمن العام اضطلعت بها في السابق، ومهاماً إضافية لم تكن تدخل على الإطلاق في نطاق مهام قوات الأمن التابعة للدولة (انظر الوثيقة A/74/244).

33 - وتستعين الدول بمصادر خارجية في تقديم خدمات الفضاء الإلكتروني إلى جهات فاعلة غير تابعة لها لعدد من الأسباب. وبنفس الطريقة التي تنقصر بها الدول في كثير من الأحيان إلى القدرات اللازمة لاستخدام أساليب الحرب التقليدية، قد لا تمتلك بعض الدول قدرات إلكترونية كافية، لا سيما بالنظر إلى أن التكنولوجيا ذات الصلة تتطور باستمرار وتتطوي على تكلفة كبيرة. وبالمثل، قد لا تتمكن الدول من الاحتفاظ بهذه القدرات الإلكترونية، وبالتالي قد تفضل الاستعانة بمصادر خارجية حسب الحاجة. والطلب على قدرات الفضاء الإلكتروني آخذ في الازدياد<sup>(28)</sup>. وتزامن مع نقص واسع النطاق في الطاقات والقدرات داخل الدول، ونجم عنه<sup>(29)</sup>. والانتقال إلى توظيف جهات فاعلة من القطاع الخاص أو الاستعانة بمصادر خارجية في بعض الدول يرتبط بانخفاض ميزانيات الدفاع والاتجاه الأعم نحو إشراك القطاع الخاص في توفير خدمات عامة ستشمل عمليات عسكرية وخدمات أمنية<sup>(30)</sup>. وعلاوة على ذلك، يمكن أن تتيح هذه الاستعانة بمصادر خارجية للدول أن تتأى بنفسها عن الأنشطة في الفضاء الإلكتروني وتتجنب التدقيق والعواقب<sup>(31)</sup>.

34 - ويشير الفريق العامل إلى صعوبة تحديد أمثلة معينة بأي قدر من اليقين تستخدم فيها الدول مرتزقة وجهات فاعلة ذات صلة بالمرتزقة وتستعين بمصادر خارجية لتوفير خدمات إلكترونية لجهات من غير الدول. ومن الصعب أيضاً التأكد من نطاق توفير هذه الخدمات وطبيعتها على وجه الدقة، نظراً للطبيعة البالغة الحساسية لهذه العمليات والسرية والغموض اللذين يكتنفان صناعة الفضاء الإلكتروني. ويلزم إجراء مزيد من البحوث لتحديد الجهات الفاعلة وأنواع الخدمات التي تقدمها<sup>(32)</sup>. والبحوث الجارية بشأن كيفية تعاقد الجهات من الدول ومن غير الدول على توفير القدرات الإلكترونية ونوع الخدمات التي تشتريها بحوث غير مكتملة ومشوبة بالعيوب في آن واحد. ويعزى عدم اكتمال الصورة إلى عدد من العوامل، منها أن معظم الشركات العاملة في هذا المجال شركات خاصة (غير مدرجة في البورصة)<sup>(33)</sup>.

35 - غير أن المعلومات الواردة تشير بقوة إلى أن هذا التعاقد والاستعانة بمصادر خارجية مستمران وسيستمران في المستقبل. ومن المناسب أيضاً أن نفترض أنهما يحدثان نظراً للنمو الهائل لصناعة الخدمات الإلكترونية، وأنه قبل توسع دور أنشطة الفضاء الإلكتروني، كانت الدول تستعين بجهات من غير الدول للاضطلاع بالمهام الأمنية والوظائف العسكرية التقليدية. ولا تستطيع الحكومة عادة مواكبة الوتيرة التي يطور بها القطاع الخاص التكنولوجيات الجديدة<sup>(34)</sup>. وفي سياق التطورات التكنولوجية السريعة والاستثمارات في التكنولوجيات الرقمية والذكاء الاصطناعي، يعتقد الفريق العامل اعتقاداً راسخاً أنه ستستمر الاستعانة بالجهات من غير الدول لتوفير الخدمات والمنتجات في الفضاء الإلكتروني.

(28) انظر المساهمة التي قدمها كيرغ، الصفحة 1.

(29) المرجع نفسه.

(30) مساهمة مقدمة تحت الختم.

(31) انظر المساهمة التي قدمها كيرغ، الصفحة 1.

(32) انظر المساهمة التي قدمتها مؤسسة تكنولوجيا المعلومات والاتصالات من أجل السلام، الصفحة 2.

(33) انظر المساهمة التي قدمتها مؤسسة The Citizen Lab، الصفحة 1.

(34) انظر المساهمة التي قدمتها مؤسسة تكنولوجيا المعلومات والاتصالات من أجل السلام، الصفحة 2.

36 - والهجمات الإلكترونية متعددة المراحل والخطوات، وبالتالي يصعب للغاية عزو المسؤولية عنها إلى مرتكبيها وعملائهم. ففي هجوم على شبكة الحواسيب المصابة، مثلاً، يتسلل المسؤول عن الروبوت إلى شبكة كبيرة من الحواسيب الضعيفة ويوجه شبكة الحواسيب المعرضة للخطر لمهاجمة شبكة الضحايا. وقد يمتد تتبع الهجوم إلى المسؤول عن الروبوت عبر عدة بلدان وعدة ولايات قضائية<sup>(35)</sup>. ويثير ذلك شواغل كبيرة حيث يُحتمل أن تؤدي العمليات السيبرانية إلى المساس بحقوق الإنسان بدرجة كبيرة. ومن دواعي القلق الأخرى أن وكلاء الإنترنت قد ينتقلون عبر الحدود، فيفلتون من آليات الرقابة التنظيمية والمساءلة<sup>(36)</sup>.

37 - وبدأت الدول والجهات من غير الدول في استخدام جهات من القطاع الخاص لفرض قوتها في الفضاء الإلكتروني، بالنظر إلى التكلفة المنخفضة نسبياً لهذه العمليات مقارنة بالحرب التقليدية وإمكانية الاستتار وراء جهة يصعب جداً كشف هويتها. ويتيح استخدام وكيل تحقيق درجة واحدة من الفصل بين مرتكب الهجوم وهدفه، ويستفيد المهاجم أيضاً من درجة عالية من إمكانية إغفال الهوية المتاحة على الإنترنت والتحديات المتعلقة بكيفية إسناد المسؤولية عن العملية السيبرانية في الوقت المناسب<sup>(37)</sup>. وتعتمد الفائدة من استخدام هذه الجهات على أنها، بخلاف الدول التي تخضع لبروتوكولات القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني، تعمل خارج نطاق هذه البروتوكولات، مما يجعل إسناد المسؤولية والتوقيف والملاحقة القضائية أمراً صعباً<sup>(38)</sup>. فذلك يتيح للدولة بدورها أن تتأى بنفسها عن العمليات السيبرانية، وبالتالي أن تتجنب التدقيق وإسناد المسؤولية والتتبع<sup>(39)</sup>.

#### رابعاً - تنظيم دور المرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة والشركات العسكرية والأمنية الخاصة ومشاركتها في توفير الخدمات الإلكترونية

38 - إن تنظيم دور المرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة والشركات العسكرية والأمنية الخاصة في توفير الخدمات في الفضاء الإلكتروني، بما في ذلك الهجمات الإلكترونية والحرب الإلكترونية، على الصعيد الدولي، يطرح عدداً كبيراً من التحديات والصعوبات. وتتعلق هذه التحديات والصعوبات، على وجه الخصوص، بما يلي: (أ) تصور ما يشكل أنشطة سيبرانية، بما في ذلك الحرب الإلكترونية والهجمات الإلكترونية؛ (ب) تحديد مصدر الهجمات الإلكترونية وسائر الأنشطة الإلكترونية؛ (ج) عزو هذه الهجمات أو الأنشطة إلى أشخاص أو كيانات معينة؛ (د) تحديد العلاقة بين الجهة من غير الدول والدولة التي تنفذ هذه الأنشطة نيابة عنها، إن كان الحال كذلك أصلاً، ومسألة ما إذا كانت أنشطة إلكترونية معينة تشكل ضلوعاً أو مشاركة مباشرة أو غير مباشرة في الأعمال العدائية الجارية. ويدور نقاش وجدل كثير يركز على مدى التنظيم الحالي للأنشطة الإلكترونية ومدى ضرورة تنظيمها على الصعيد الدولي.

(35) David D. Clark and Susan Landau, "Untangling attribution", *Harvard National Security Journal*, vol. 2, No. 2 (2011).

(36) Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018).

(37) انظر المساهمة التي قدمتها الرابطة النسائية الدولية للسلم والحرية، الصفحة 4.

(38) Ataa Dabour, "The rise of cyber-mercenaries", 2021، متاح عبر الرابط التالي: [www.hscentre.org/technology/the-rise-of-cyber-mercenaries/](http://www.hscentre.org/technology/the-rise-of-cyber-mercenaries/)

(39) انظر المساهمة التي قدمتها مؤسسة تكنولوجيا المعلومات والاتصالات من أجل السلام، الصفحة 2.

- 39 - وهذه التحديات ناجمة عن الغموض الذي تتسم به الانتهاكات في الفضاء الإلكتروني ومصدرها والكيانات التي تقوم بها، والعلاقة بين الدول والجهات الأخرى من غير الدول. وهذا الفصل، الذي لا يمكن تحقيقه بسهولة في سياق النزاع المسلح الحركي التقليدي، يفيد الجهات من الدول ومن غير الدول، لأنه قد يحمي كلاهما من المسؤولية عن أفعالها؛ إلا أنه يجعل تنظيم هذه الأنشطة أصعب بكثير. ومن الواضح أن مسألة عزو العمليات السيبرانية ومسألة الفصل المعتمد لهذه العمليات عن القوات المسلحة التابعة للدولة، بحيث يمكن أن يكون هناك "إنكار مقبول"، تمثلان مشكلة جدية في النهوض بالضوابط التنظيمية.
- 40 - ويشمل الإطار التنظيمي الدولي الحالي ذي الصلة ميثاق الأمم المتحدة، والقانون الدولي الإنساني، ودليل تالين للقانون الدولي المنطبق على حرب الفضاء الإلكتروني، والقانون الجنائي الدولي، والقانون الدولي لحقوق الإنسان، والقانون غير الملزم، والقانون الوطني.

### ألف - ميثاق الأمم المتحدة

- 41 - ينبغي أن يؤدي ميثاق الأمم المتحدة، ولا سيما المادة 2 (4)، التي تحظر التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة، دوراً في تنظيم أنشطة الفضاء الإلكتروني والمراقبة عليها، بما في ذلك أنشطة المرتزقة. ويستند ذلك إلى أن أنشطة الفضاء الإلكتروني قد يكون حجمها وتأثيرها بحيث تشكل "استخداماً للقوة" وبالتالي قد تكون محظورة بموجب ميثاق الأمم المتحدة. ويمكن أيضاً أن تبلغ هذه الأنشطة عتبة "هجوم مسلح" يؤدي إلى إعمال حق الدولة في اتخاذ إجراءات للدفاع عن نفسها، عملاً بالمادة 51 من ميثاق الأمم المتحدة. ومسألة ما إذا كانت هذه الأنشطة الإلكترونية تستوفي العتبات ذات الصلة، لا سيما فيما يتعلق بمبدأي الضرورة والتناسب، هي مسألة واقع ودرجة، ولكن ما من شك في أنها يمكن أن تستوفي هذه العتبات في ظروف معينة، بالنظر إلى طبيعة الأنشطة الإلكترونية الحديثة وآثارها<sup>(40)</sup>.
- 42 - بيد أن هناك مسألة أصعب ينبغي النظر فيها، وهي ما إذا كانت الهجمات الإلكترونية أو الأنشطة الأخرى التي تقوم بها جهات من غير الدول تستوجب سريان الأحكام ذات الصلة من ميثاق الأمم المتحدة. ويتوقف الجواب على ما إذا كانت أفعال هؤلاء الأفراد أو الكيانات تُسند إلى دولة معينة بمقتضى مشاريع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً، نظراً لأن ميثاق الأمم المتحدة لا ينطبق إلا على الحالات التي تحدث بين الدول ذات السيادة.
- 43 - وقد تطرح مسألة العزو تحديات كبيرة من ناحية الإثبات بالنظر إلى أن الكيانات التي تقدّم خدمات متعلقة بأنشطة الفضاء الإلكتروني كثيراً ما تعمل باستقلالية كبيرة عن الدولة، وقد يكون من الصعب أو المستحيل تتبع مصدر الهجمات الإلكترونية نظراً لأنها تجرى عن بعد وقد تتألف من مدخلات مختلفة من مواقع وجهات فاعلة مختلفة. وتستخدم عمداً، بطبيعة الحال، آليات لتجنب رصد الهجمات وعزوها.

(40) انظر الرابط التالي: <https://international-review.icrc.org/articles/can-jus-ad-bellum-override-jus-bello-reaffirming-separation-two-bodies-law>

## باء - القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني

44 - الدول ملزمة باحترام القواعد الدولية لحقوق الإنسان، سواء وقت السلم أو أثناء النزاع المسلح، مع مراعاة الاستثناءات والتقييدات الجزئية المحددة ذات الصلة. ويتعين على الدول أيضا ضمان امتثال الجهات الفاعلة الخاصة داخل إقليمها من خلال القانون الوطني وإنفاذه. والإطار الشامل الذي أعد بعناية لحماية حقوق الإنسان على الصعيد الدولي، بما يضم من معاهدات وهيئات رصد وآليات إنفاذ مختلفة، هو وسيلة جاهزة لتنظيم الفضاء الإلكتروني.

45 - وأكدت اللجنة الدولية للصليب الأحمر في البيان الذي ألقته أمام الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، أن قواعد القانون الدولي الإنساني تنطبق على أشكال النزاع المسلح الجديدة، بما في ذلك الحرب الإلكترونية<sup>(41)</sup>. ولدى التوصل إلى ذلك الاستنتاج، يستند إلى فتوى محكمة العدل الدولية في القضية المتعلقة بشرعية الأسلحة النووية أو استخدامها، التي خلصت فيها المحكمة إلى أن القانون الدولي الإنساني ينطبق على الأسلحة وأنواع الحرب الحالية والمستقبلية<sup>(42)</sup>. ولئن كان هناك نقاش مستمر بشأن تفسير محدد فيما يتعلق بتطبيق مبادئ القانون الدولي الإنساني ذات الصلة على العمليات السيبرانية في سياق النزاع المسلح، يبدو أن القواعد تنطبق من حيث المبدأ. وتؤكد هذا النهج في دليل تالين للقانون الدولي المنطبق على حرب الفضاء الإلكتروني. فالدليل ينص بشكل قاطع على أن "قانون النزاعات المسلحة ينطبق على العمليات السيبرانية كما ينطبق على العمليات الأخرى التي تتم في سياق نزاع مسلح".

46 - غير أن هذا النهج، مرة أخرى، لا يخلو من الصعوبات، لا سيما في ضوء دور الجهات من غير الدول التي تقدم هذه الخدمات في الفضاء الإلكتروني. ولا يوجد تعريف متفق عليه دوليا لما يشكل هجوما إلكترونيا أو أعمالا عدائية إلكترونية في إطار القانون الدولي الإنساني. إلا أن مفهوم "الهجوم" نفسه ذو أهمية، ولا سيما فيما يتعلق بمبدأ التمييز وبما يشكل أهدافا عسكرية ومدنية. وقد يكون الطابع العسكري أو المدني للأهداف مادة للتفسير، ولكن هذا التفسير لا يعتمد على أسلوب الحرب المستخدم أثناء الهجوم. وسواء نُفذ الهجوم بوسائل حربية حركية أو بواسطة تكنولوجيات إلكترونية، ينبغي احترام الطابع المدني للهدف.

47 - وثمة مسألة أخرى تثير القلق وهي حالة العمليات السيبرانية أثناء النزاع المسلح، وعلى الأخص تحديد ما إذا كانت العملية تشكل مشاركة مباشرة في الأعمال العدائية، وهو ما يكتسي أهمية في استيفاء معايير تصنيف الأشخاص كمرتزقة بمقتضى المادة 47 من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام 1949، أو ما إذا كانت العملية صلة كافية بالنزاع المسلح المعين. وفي بعض الحالات، تكون الهجمات الإلكترونية الموجهة لتدمير قدرات الدولة والهياكل الأساسية للدولة معادلة لمشاركة جهة من غير الدول

(41) بيان ألقته فيرونك كريستوري، كبيرة المستشارين لشؤون تحديد الأسلحة لدى اللجنة الدولية للصليب الأحمر أمام الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، نيويورك، 10 أيلول/سبتمبر 2019.

(42) فتوى مشروعية التهديد بالأسلحة النووية أو استخدامها، تقارير محكمة العدل الدولية لعام 1996، صدرت في 8 تموز/يوليه 1996؛ اللجنة الدولية للصليب الأحمر، ورقة موقف بشأن القانون الدولي الإنساني والعمليات السيبرانية خلال النزاع المسلح، تشرين الثاني/نوفمبر 2019، الصفحة 4.

مشاركة مباشرة في الأعمال العدائية في سياق نزاع مسلح<sup>(43)</sup>. واحتمال أن يؤثر أي نشاط إلكتروني معين على القدرة العسكرية لطرف في نزاع ما، وأن يسبب ضررا لطرف في نزاع ما، مع وجود صلة كافية بين الفعل والنزاع المسلح، يتوقف على وقوعه ودرجته. فهذه المسألة، إضافة إلى الجوانب القانونية، لها بعدٌ عملي أكثر، إذ قد لا يكون من الممكن دائما تحديد وقوع هجمات إلكترونية أو أنشطة إلكترونية غير ملحوظة. ومن المرجح أن يتوقف تفسير جميع المفاهيم على ممارسات الدول.

48 - وفيما يتعلق بالمرتزقة على وجه التحديد، لا يحق للأشخاص الذين يستوفون تعريف المرتزق أن يتمتعوا بمركز المقاتل وتدابير الحماية المرتبطة به أصلا. والأهم من ذلك، يمكن حاليا مقاضاتهم على مجرد أنهم شاركوا في الأعمال العدائية، بغض النظر عما إذا كانت دولة أو جهة من غير الدول قد تعاقدت معهم للمشاركة في الأعمال العدائية (السيبرانية). ويمكن أيضا مقاضاتهم على أنهم شاركوا في أنشطة المرتزقة شريطة أن يحدد النظام المحلي المعني هذه الأحكام القانونية. وعلاوة على ذلك، وفقا للمادة 1 المشتركة من اتفاقيات جنيف لعام 1949، تلتزم الدول بضمان احترام الاتفاقية، ويشمل ذلك ضمان أن تتصرف الكيانات التي تعمل نيابة عنها والتي يمكن أن تشمل جهات من غير الدول تعمل نيابة عن الدول، وفقا للقانون الدولي الإنساني.

49 - ونتيجة لذلك، أشير إلى أن التعريف التقليدي للمرتزق قد لا يكون مناسباً لتطور وسائل الحرب والنزاعات المعاصرة التي تتسم باستخدام الحرب الإلكترونية أو غيرها من الأنشطة الإلكترونية أو تنطوي عليها، على الأقل، مما يشير إلى ضرورة إعادة تصور فهم ما يشكل مرتزقا داخل الفضاء الإلكتروني<sup>(44)</sup>.

50 - وهناك مسألة أخرى تنشأ، ويتعين النظر فيها فيما يتعلق بتطبيق القانون الدولي الإنساني على الفضاء الإلكتروني، وهي تتعلق بمختلف النظم القانونية التي تنطبق على النزاعات المسلحة غير الدولية والدولية، وما إذا كان ينبغي اتباع نفس النهج فيما يتعلق بخدمات الفضاء الإلكتروني. والسؤال المطروح أيضا هو ما إذا كان يمكن الحفاظ على التمييز التقليدي، بالنظر إلى تطور الحرب الإلكترونية والهجمات الإلكترونية.

51 - وإضافة إلى ذلك، هناك مسألة أساسية تتبع من أن القانون الدولي الإنساني، وإن كان يوفر إطارا تنظيميا متطورا وشاملا يمكن تطبيقه على الأنشطة الإلكترونية، فإنه بالطبع لا ينطبق إلا في أوقات النزاع المسلح. والحال هو أن العديد من الأنشطة الإلكترونية، وربما أغليبتها، تجري خارج سياق نزاع مسلح، وبالتالي لا ينطبق عليها النظام التنظيمي للقانون الدولي الإنساني.

## جيم - القانون الجنائي الدولي

52 - ينطبق القانون الجنائي الدولي على أي شخص طبيعي يرتكب جريمة دولية، وللمحكمة الجنائية الدولية اختصاص في جرائم الحرب والجرائم ضد الإنسانية والإبادة الجماعية والحرب العدوانية. ولذلك، إذا استوفت الخدمات الإلكترونية التي يقدمها أشخاص طبيعيون عنصرا واحدا أو أكثر من عناصر جريمة واحدة أو أكثر، واستوفيت معايير أخرى ذات صلة، يمكن أن يكون للمحكمة الجنائية الدولية اختصاص على

(43) Nils Melzer, *Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (Geneva, ICRC, May 2009). متاح على الرابط التالي: [www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf](http://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf)

(44) انظر المساهمة التي قدمها فان دير واغ - كاولينغ، وفان نيكريك، والدكتور راملوكان، الصفحة 4.



الأفعال الإجرامية التي يرتكبها المرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة في الفضاء الإلكتروني. ويمكن أن يكون القانون الجنائي الدولي مفيداً بقدر ما يمكن أن يساعد مبدأ مسؤولية القادة في التغلب على بعض العقبات المتصلة بالتعرف على الجاني الفعلي وتحديد مكانه. وينبغي لرؤساء الأفراد المتورطين في ارتكاب الجريمة، بطرق مثل الأمر بارتكاب هجمات إلكترونية مدمرة أو عدم الحيلولة دون هذه الهجمات الإلكترونية الخبيثة، ألا يفلتوا من المساءلة<sup>(45)</sup>. وإضافة إلى التحديات التي سبق تحديدها أعلاه، يقتضي القانون الجنائي الدولي إثبات الجرائم في الإجراءات الدولية بما لا يدع مجالاً للشك، وهو أعلى معايير الإثبات. وعلاوة على ذلك، بالنظر إلى أن العمليات السيبرانية قد تتعلق بعدة دول، قد تنشأ مسائل متعلقة بالولاية القضائية والتكامل، وقد يطرح ذلك تحديات إضافية في التحقيقات والملاحقات القضائية.

53 - والاتفاقية الدولية لمكافحة تجنيد المرتزقة واستخدامهم وتمويلهم وتدريبهم، واتفاقية منظمة الوحدة الأفريقية للقضاء على أعمال المرتزقة في أفريقيا، كلتا هاتين التجزئتين الارتزاق، مما يضع أساساً قانونياً بديلاً لمقاضاة الأنشطة المتصلة بالمرتزقة ومعاقبته. وينبغي للدول التي تصدق على هذه الاتفاقيات أن تدرج الحكم ذي الصلة في نظمها القانونية الداخلية، مما يمكن المحاكم المحلية من مقاضاة أنشطة المرتزقة.

## دال - القانون غير الملزم والمبادرات الجارية

54 - إضافة إلى أطر القانون الدولي الملزمة، ظهر خلال العقد الماضي عدد من المبادرات المتعددة الجهات والأطراف التي تستهدف مختلف الجهات الفاعلة وتسعى إلى تعزيز السلوك المسؤول أثناء استخدام تكنولوجيا المعلومات والاتصالات. وهذه الأطر تشمل الأطر المعيارية غير الملزمة التي تستهدف الجهات الفاعلة من القطاع الخاص مثل اتفاقية تكنولوجيا الأمن السيبراني وميثاق الثقة الذي وضعتة شركة Siemens. وقامت أفرقة خبراء مستقلة مثل اللجنة العالمية المعنية باستقرار الفضاء الإلكتروني والفريق المستقل للخبراء الذي صاغ دليل تالين بوضع توصيات بشأن القواعد والقانون الدولي المنطبق. وكانت مبادرات أخرى اتخذتها جهات معنية متعددة، مثل نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني، موجهة إلى القطاع الخاص والمجتمع المدني والحكومات.

55 - وعلى مستوى مجلس حقوق الإنسان، يؤدي فريق عامل حكومي دولي مفتوح العضوية دوراً هاماً في إعداد محتوى إطار تنظيمي دولي بشأن تنظيم أنشطة الشركات العسكرية والأمنية الخاصة ورصدها والرقابة عليها. ونظراً للتغير السريع في سياقات التشغيل والخدمات المقدمة، ينبغي لأي آلية تنظيمية يتم وضعها من خلال هذه العملية أن تشير إلى "الخدمات" أو "الأنشطة" بدلاً من "الشركات العسكرية والأمنية الخاصة" باعتبارها خيارات اصطلاحية أكثر فعالية للإحاطة بانتهاكات حقوق الإنسان أو القانون الدولي الإنساني<sup>(46)</sup>.

56 - وأنشأت الجمعية العامة مؤخراً فريقين لمناقشة المسائل أوسع نطاقاً المتعلقة بالأمن في مجال تكنولوجيا المعلومات والاتصالات، ويمكن أن يقدم كلاهما إرشادات في هذا الصدد، وهما: الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلوكية واللاسلكية في سياق الأمن الدولي (انظر قرار الجمعية العامة 27/73)، وفريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول

(45) انظر المساهمة التي قدمتها منظمة الوصول الآن، الصفحة 10.

(46) انظر البيان الذي أدلت به يلينا أباراك، رئيسة الفريق العامل المعني باستخدام المرتزقة. متاح عبر الرابط التالي:

[www.ohchr.org/EN/HRBodies/HRC/IGWG\\_PMSCs/Pages/Session2.aspx](http://www.ohchr.org/EN/HRBodies/HRC/IGWG_PMSCs/Pages/Session2.aspx)

المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي (انظر قرار الجمعية العامة 266/73). وتنتظر كلتا العمليتين في ستة مجالات رئيسية، منها التهديدات القائمة والمحتملة؛ وقواعد ومعايير ومبادئ السلوك المسؤول للدول والقانون الدولي؛ وتدابير بناء الثقة؛ وبناء القدرات؛ والحوار المؤسسي المنتظم.

57 - وفي آذار/مارس 2021، اعتمد الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي تقريراً بتوافق الآراء عرض فيه بعض التوصيات غير الملزمة لجميع الدول الأعضاء. وفي حين أن أياً من هذه التوصيات لا تتناول مسألة المرتزقة أو الجهات الفاعلة ذات الصلة بالمرتزقة، يتضمن التقرير عدة إشارات إلى حقوق الإنسان، ويسلم في التقرير بأن بعض الجهات من غير الدول قد أثبتت وجود قدرات في مجال تكنولوجيا المعلومات والاتصالات لم تكن متاحة من قبل إلا للدول. وأشار في التقرير إلى أن استمرار تزايد الحوادث التي تنطوي على استخدام خبيث لتكنولوجيا المعلومات والاتصالات من جانب جهات من الدول ومن غير الدول اتجاهاً يبعث على القلق (انظر الوثيقة A/AC.290/2021/CRP.2، الفقرة 16). وقررت الجمعية العامة في قرارها 240/75 المؤرخ 31 كانون الأول/ديسمبر 2020 عقد اجتماع لفريق عامل جديد مفتوح العضوية حتى عام 2025، ويعتقد الفريق العامل المعنى بمسألة استخدام المرتزقة وسيلة لانتهاك حقوق الإنسان وإعاقة ممارسة حق الشعوب في تقرير مصيرها أن ذلك يتيح فرصة هامة لمناقشة مسألة المرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة العاملة في الفضاء الإلكتروني.

58 - وأكد فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي من جديد، في التقرير الذي أعده بتوافق الآراء لعام 2021، أنه "يجب على الدول ألا تستخدم وكلاء عنها لارتكاب أفعال غير مشروعة دولياً باستخدام تكنولوجيا المعلومات والاتصالات، وينبغي أن تحرص على ألا تستخدم جهات من غير الدول إقليمياً لارتكاب أفعال من هذا القبيل"<sup>(47)</sup>. ولئن كان ذلك لا يضع معياراً قانونياً للدول، فإنه يدين فعلاً تنتسب الدول ومعاينة الوكلاء. وأشار فريق الخبراء الحكوميين إلى أن الجهود التي تبذلها الدول لتعزيز احترام حقوق الإنسان ومراعاتها وكفالة استخدام تكنولوجيات المعلومات والاتصالات استخداماً مسؤولاً ومأموناً ينبغي أن تكون جهوداً متكاملة ومتراصة يعزز بعضها بعضاً، مع التسليم بأن المراقبة الجماعية قد تكون ذات آثار سلبية على حقوق الإنسان، بما في ذلك الحق في الخصوصية<sup>(48)</sup>.

59 - ووصفت المبادرات الناشئة لوضع المعايير بأنها تشكل "مجمع نظم" للأمن السيبراني ينطوي على ترتيب الجهود بدلاً من صك واحد ملزم تراتبي.

## خامساً - الآثار في مجال حقوق الإنسان

60 - لا يمكن إنكار أن الأنشطة السيبرانية تمس معايير وقواعد حقوق الإنسان، وأن لها القدرة على التسبب في انتهاكات أثناء النزاعات المسلحة وفي وقت السلم على حد سواء، وبالتالي تمس مجموعة متنوعة من الحقوق. ويذكر الفريق العامل باستنتاجاته التي مفادها أن المخاطر والآثار الجنسانية الناجمة

(47) انظر الرابط التالي: [https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-](https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf)

(g) para. 71. [advance-copy.pdf](#).

(48) المرجع نفسه، الفقرتان 39 و 37.

عن الأنشطة التي تضطلع بها الشركات العسكرية والأمنية الخاصة لها قواسم مشتركة عديدة بصرف النظر عن حجمها والخدمات المقدمة (انظر الوثيقة A/74/244، الفقرة 6). وإضافة إلى ذلك، حدد الفريق العامل فئات تتأثر بشكل خاص بالمرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة التي تستعين بها الدول، مثل المدافعين عن حقوق الإنسان والمهاجرين وقادة المعارضة والصحفيين، والمثليات والمثليين ومزدوجي الميل الجنسي ومغايري الهوية الجنسية وحاملي صفات الجنسين والأشخاص غير المتقيدين بالتميطات الجنسية في سياق العنف الجنساني.

61 - ويمكن أن تكون لأشكال الحرب الجديدة والناشئة تأثير كبير على كل من الأهداف العسكرية والسكان المدنيين، ويمكن أن تؤدي إلى انتهاكات للقانون الدولي الإنساني ولحقوق الأفراد وحياتهم في سياق النزاعات المسلحة وبطريقة أخرى. وسبق أن أشار الفريق العامل إلى أن الحرب السيبرانية قد اعتُرف بأنها أسلوب من أساليب الحرب التي لا تقتصر قدراتها على التسلل أو التعطيل أو إلحاق الضرر بالأهداف العسكرية أو الأعيان المدنية أو حتى تدميرها فحسب، بل تستطيع أيضاً أن تسبب أضراراً بشرية فادحة<sup>(49)</sup>. ويمكن أن يكون للتخريب الإلكتروني آثار ثانوية هائلة على عمل البنية التحتية الحيوية، مما قد يقوض الصحة العامة والسلامة والأمن. وفي هذا السياق، فإن الحق في الحياة والحق في عدم التعرض للتعذيب وغيره من ضروب المعاملة اللاإنسانية أو المهينة هما الحقان الرئيسيان المعرضان لخطر الانتهاك من خلال العمليات السيبرانية.

### الحق في الخصوصية وحرية التعبير

62 - في جميع السياقات، يتعرض الحق في الخصوصية والحق في حرية التعبير لخطر الانتهاك. وعندما يُستخدم المرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة لمهاجمة الدول، فإنهم يصبحون دائماً الأدوات الرئيسية لتقويض سيادة هذه الدول وسلامتها الإقليمية، مما يعوّق أيضاً ممارسة الحق في الخصوصية.

63 - ويمكن أيضاً أن يتعرض الحق في الخصوصية للخطر من خلال الرصد وجمع المعلومات الاستخبارية. وثمة شواغل كبيرة بشأن العمليات السيبرانية التي تستهدف المجتمع المدني، وبخاصة المدافعون عن حقوق الإنسان والصحفيون، من أجل تعطيل أنشطتهم بهدف خنق المعارضة وزيادة سيطرة الدولة على سكانها. وعلى الرغم من أن الحكومات تستخدم منذ زمن طويل أساليب مختلفة لمراقبة وتعقب مواطنيها والمخالفين معها في الرأي ومعارضيه السياسيين والمدافعين عن حقوق الإنسان، فإن الأدوات التكنولوجية المتاحة الآن، مثل البرمجيات الخبيثة وبرامج التجسس، تتيح لها القيام بذلك بتكلفة أقل وتوسيع النطاق الجغرافي للمراقبة وزيادة نطاقها وحجمها، مما يمكن الحكومات من تنفيذ القمع الرقمي على نحو أكمل من أي وقت مضى<sup>(50)</sup>. وبعض أشكال برامج التجسس أمثلة نموذجية على الأدوات التي تتيح مراقبة الأهداف عن بعد<sup>(51)</sup>.

(49) اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة"، ورقة موقف، تشرين الثاني/نوفمبر 2019.

(50) انظر المساهمة التي قدمتها مؤسسة The Citizen Lab، الصفحة 8.

(51) A/HRC/41/35، para. 9; Bill Marczak and others, *Hide and seek: tracking NSO Group's Pegasus spyware to operations in 45 countries*, Citizen Lab, 18 September 2018.

64 - وعلاوة على ذلك، أشير إلى أن الحق في حرية التعبير يمكن انتهاكه من خلال الرقابة التي تمارسها بعض الدول على محتوى الإنترنت أو عن طريق نشر المعلومات المضللة والمعلومات الخاطئة. والعمليات السيبرانية التخريبية التي يقوم بها أو يتعاقد عليها عملاء حكوميون يمكن أن تقوض سلامة الفضاء الإلكتروني وحرية التعبير والحريات المدنية الأخرى ليس للأفراد فحسب، بل للفئات والمجتمعات بأسرها<sup>(52)</sup>. كما أن المراقبة المحددة الهدف تنشئ حوافز للرقابة الذاتية، وتقوض بشكل مباشر قدرة الصحفيين والمدافعين عن حقوق الإنسان على إجراء التحقيقات وإقامة علاقات مع مصادر المعلومات والحفاظ عليها<sup>(53)</sup>.

65 - وتكنولوجيا المراقبة التي تطورها شركات خاصة وتتعهدها وأحيانا تديرها تؤدي أيضا دورا أساسيا في تحويل مسارات الهجرة بعيدا عن المناطق التي يمكن اكتشافها وإلى مناطق خارج نطاق التغطية بمعدات المراقبة. وبالتالي يُضطر المهاجرون إلى سلوك طرق غير مباشرة وأكثر خطورة في رحلات الهجرة بحرا أو برا، مما يزيد من صعوبة التحرك والآثار الفسيولوجية والعقلية ويؤدي إلى ألم ومعاناة يفضيان في كثير من الأحيان إلى الوفاة بسبب ضربات الشمس والتجفاف الحاد وغير ذلك من الآلام<sup>(54)</sup>.

66 - وتتجسد آثار القدرات السيبرانية في آثار ضارة كبيرة على كل من المؤسسات والأفراد، مما يؤثر سلبا في قدرة الحكومات على توفير الحماية وضمان رفاه شرائح كبيرة من السكان ويعرقل التمتع بحقوق الإنسان. فالهجمات على النظم الانتخابية، مثلا، تؤثر مباشرة على الحقوق الديمقراطية الأساسية لتمثيل المواطنين الذين يُحرمون من حقهم في التصويت. وأفيد أيضا بأن بعض البلدان تشن هجمات إلكترونية روتينية على المناطق المدنية، أو تخترق الشركات الخاصة، أو تقوض الجيوش الأجنبية، وتستخدم أدوات على الإنترنت للتلاعب بالمعلومات أو الدعاية الرقمية لتشكيل آراء الآخرين، وتستخدم مرتزقة رقميين للقيام بهذا العمل<sup>(55)</sup>.

67 - وهناك تقارير عن هجمات إلكترونية تسببت في أضرار مادية واسعة النطاق، بما في ذلك أضرار في شبكات الكهرباء والمؤسسات المالية والوزارات الحكومية<sup>(56)</sup>. ويمكن أن يؤدي تدمير قواعد البيانات التي تتضمن معلومات متعلقة بالمدنيين إلى توقف تام للخدمات الحكومية والأعمال التجارية الخاصة بسرعة، وبالتالي إلحاق ضرر بالمدنيين أكبر من تدمير الأعيان المادية<sup>(57)</sup>.

(52) S/2021/569، الفقرة 103.

(53) انظر الوثيقة A/HRC/38/35/Add.2، الفقرة 53؛ والوثيقة A/HRC/41/35، الفقرة 26.

(54) A/HRC/45/9، الفقرتان 44 و 45.

(55) Paul D. Shinkman, "America Is losing the cyber war", U.S. News and World Report website, 29 September 2016، متاح على الرابط التالي: [www.usnews.com/news/articles/2016-09-29/cyber-wars-how-the-us-stacks-up-against-its-digital-adversaries](http://www.usnews.com/news/articles/2016-09-29/cyber-wars-how-the-us-stacks-up-against-its-digital-adversaries).

(56) Neri Zilber, "The rise of the cyber-mercenaries: what happens when private firms have cyberweapons as powerful as those owned by governments?", *Foreign Policy* (FP), 31 August 2018، متاح على الرابط التالي: <https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/>.

(57) اللجنة الدولية للصليب الأحمر، "القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة"، ورقة موقف، تشرين الثاني/نوفمبر 2019.

## تقرير المصير

68 - فيما يتعلق بالحق في تقرير المصير، يمكن لشركات الأمن السيبراني أن تعوق إلى حد كبير ممارسة حق الشعوب في تقرير مصيرها، وذلك باستخدام منتجات وخدمات عسكرية وأمنية في الفضاء الإلكتروني. ولهذه الجهات الفاعلة القدرة على التأثير على حركات التمرد المحلية بطرق يمكن أن تقوض في نهاية المطاف الحق في تقرير المصير (انظر الوثيقة A/71/318، الفقرة 20).

## سادسا - استنتاجات وتوصيات

69 - يؤثر تطوير التكنولوجيات ورقمنتها تأثيرا مباشرا على جميع مجالات الحياة المدنية. كما يعتمد المجال العسكري بشكل متزايد على التكنولوجيات الرقمية. وينعكس الاتجاه المتزايد نحو الرقمنة في زيادة التقارب بين الفضاء المعلوماتي والفضاء الإلكتروني ويمكن أن يكون له آثار سلبية على السكان في أوقات السلم وأثناء النزاعات المسلحة.

70 - وأخذ الفريق العامل في الاعتبار تطور توفير المرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة وشركات الأمن العسكري الخاصة للمنتجات والخدمات العسكرية والأمنية في الفضاء الإلكتروني وما يترتب على ذلك من عواقب على التمتع بحقوق الإنسان. وأشار إلى التحديات التي ينطوي عليها التركيز حصرا على الأنشطة التي تستوفي تعريف "المرتزق" في الإطار القانوني الدولي المنطبق، واتبع نهجا أوسع نطاقا بدراسة مجموعة متنوعة من الجهات الفاعلة والمظاهر التي تندرج ضمن مفهوم أكثر قابلية للتكيف عن الأنشطة المتصلة بالمرتزقة.

71 - ولاحظ الفريق العامل بقلق أن بعض الدول، إما بالفعل أو الامتناع، تخفي ضلوعها في عمليات سيبرانية خبيثة، سعيا إلى اكتساب نفوذ عسكري استراتيجي بالتهرب من مسؤولياتها بمقتضى القانون الدولي، بما في ذلك عن الانتهاكات والتجاوزات التي ترتكبها جهات فاعلة غير حكومية يستعان بها لهذا الغرض. غير أن الاستعانة بجهات فاعلة خاصة لتوفير الخدمات العسكرية والأمنية في الفضاء الإلكتروني لا تعفي الدول من التزاماتها بمقتضى القانون الدولي.

72 - ولذلك فإن المظاهر الجديدة والمتطورة للأنشطة المتصلة بالمرتزقة تتطلب اهتماماً عاجلاً من الدول والجهات الأخرى المعنية. ويفصل هذا التقرير الاعتبارات التي يجب مراعاتها لدعم الدول وسائر الجهات الفاعلة عند وضع ضوابط تنظيمية للمرتزقة في الفضاء الإلكتروني بمزيد من الفعالية، بغية ضمان احترام حق الشعوب في تقرير مصيرها وحمايته وإعماله، وحماية المدنيين في حالات النزاع المسلح، وصون مبدأي عدم التدخل والسلامة الإقليمية. وينبغي أن تستند المناقشات المركزة على أي ضوابط تنظيمية إلى الإطار القانوني الدولي المتعلق بالمرتزقة، بالرغم مما يشوبه من أوجه قصور، وإطار القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان الأوسع نطاقا.

## التوصيات

73 - سعيا لمنع الآثار السلبية على حقوق الإنسان التي يسببها المرتزقة والجهات الفاعلة المرتبطة بالمرتزقة والشركات العسكرية والأمنية الخاصة في الفضاء الإلكتروني والتخفيف منها، ينبغي للدول

أن تمتنع عن تجنيد المرتزقة واستخدامهم وتمويلهم وتدريبهم، وينبغي لها أن تحظر هذا السلوك في القانون الوطني وأن تنظم الشركات العسكرية والأمنية الخاصة بفعالية.

74 - وينبغي للدول أن تلتزم بالشفافية وتحرص على تفعيلها فيما يتعلق بالتعاقد على خدمات الدعم العسكري، بما في ذلك الدعم للعمليات السيبرانية، وأن تنشر على الملأ المعلومات المتعلقة بطبيعة الخدمات وإجراءات الشراء وشروط العقود وأسماء مقدمي الخدمات بطريقة مفصلة تفصيلاً كافياً وفي الوقت المناسب. وينبغي ألا تتذرع بالشواغل الأمنية الوطنية كسبب عام لتقييد الوصول إلى هذه المعلومات؛ بل يجب أن تكون الشرعية والضرورة والتناسب مقياساً للقيود المفروضة على الوصول إلى المعلومات، متشياً مع الحق في حرية التعبير.

75 - ويتعين على الدول أن تحقق في انتهاكات القانون الدولي الإنساني وانتهاكات حقوق الإنسان المزعومة التي يقوم بها المرتزقة والجهات الفاعلة ذات الصلة بهم، وأن تحاكم مرتكبيها وتعاقبهم، وأن تتيح للضحايا سبل انتصاف فعالة. ويجب أن يُحترم ويُكفل الحق في محاكمة عادلة وفي مراعاة الأصول القانونية أثناء التحقيقات والملاحقات القضائية والمحاكمات.

76 - وعلى الصعيد الدولي، ينبغي أن تشرع الدول في إجراء حوار بشأن الأشكال الجديدة والمتطورة لأنشطة المرتزقة، لا سيما من يعملون في الفضاء الإلكتروني، بجميع أشكالها، وما تشكله من مخاطر على القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان وسبل التصدي لها بمزيد من الفعالية. وينبغي أن يشمل أي حوار من هذا القبيل المنظمات الدولية والإقليمية والمجتمع المدني والخبراء، وأن يناقش الأدوات والمبادرات القائمة.

77 - وينبغي للدول أن تقوم بتنشيط المناقشات مع الفريق العامل الحكومي الدولي المفتوح العضوية المعني بصياغة مضمون إطار تنظيمي دولي بشأن تنظيم أنشطة الشركات العسكرية والأمنية الخاصة ورصدها والرقابة عليها<sup>(58)</sup>، بما في ذلك ما يتعلق بالحالات التي تقوم فيها الشركات بتوفير خدمات سيبرانية وتعمل في سياق حرب إلكترونية. ولا بد من صك ملزم قانوناً يحكم الفضاء الإلكتروني. ومن شأن وجود إطار قانوني دولي أن يؤدي إلى التأكد وإمكانية التنبؤ عن طريق التزامات قانونية واضحة يمكن إنفاذها من خلال منندييات متخصصة لتسوية المنازعات. فتجزؤ نظم الإدارة يزيد من الالتباس التنظيمي، وكثيراً ما يضر بالبلدان النامية والجهات الفاعلة في المجتمع المدني.

78 - وينبغي أيضاً تناول الشواغل المتعلقة بحقوق الإنسان الناشئة عن مشاركة المرتزقة والجهات الفاعلة ذات الصلة بهم في العمليات السيبرانية، في إطار الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي وفريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي.

79 - وفيما يتعلق بأنشطة المرتزقة والأنشطة المتصلة بالمرتزقة والشركات العسكرية والأمنية الخاصة والمرتبطة بالجهات المسلحة من غير الدول، ينبغي أن تتفق الدول على العمليات الدولية المطلوبة لتحديد الآليات اللازمة لاعتراف أوضح وأكثر اتصافاً بالطابع الرسمي بالالتزامات الدولية للجهات المسلحة من غير الدول في مجال حقوق الإنسان وتقييم هذه الآليات ومواصلة تطويرها، بما في ذلك معايير تحديد قدرة هذه الجهات على التقيد بالالتزامات المتعلقة بحقوق الإنسان، وأن تدعم تلك العمليات.

(58) انظر قرار مجلس حقوق الإنسان 11/36.