

Distr.: General
10 July 2000
Arabic
Original: Arabic/English/Russian



الدورة الخامسة والخمسون
البند ٦٩ من جدول الأعمال المؤقت*
التطورات في ميدان المعلومات والاتصالات
السلكية واللاسلكية في سياق الأمن الدولي

التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في
سياق الأمن الدولي
تقرير الأمين العام**

المحتويات

الصفحة	
٢	أولا - مقدمة
٢	ثانيا - الردود الواردة من الحكومات
٢	الاتحاد الروسي
٧	الأردن
٨	قطر

* A/55/150.

** أعد هذا التقرير بناء على الآراء المقدمة من الدول الأعضاء.

أولا - مقدمة

١ - في الفقرتين ٢ و ٣ من القرار ٤٩/٥٤ المؤرخ ١ كانون الأول/ديسمبر ١٩٩٩ بشأن التطورات في ميدان المعلومات والاتصالات السلوكية واللاسلكية في سياق الأمن الدولي، دعت الجمعية العامة جميع الدول الأعضاء إلى إبلاغ الأمين العام بأرائها وتقييماتها بشأن المسائل التالية: (أ) التفهم العام للقضايا المتصلة بأمن المعلومات، (ب) تعريف المفاهيم الأساسية المتصلة بأمن المعلومات، بما فيها التدخل غير المأذون به في نظم المعلومات والاتصالات السلوكية واللاسلكية وموارد المعلومات أو إساءة استخدامها، (ج) استتصواب وضع مبادئ دولية يكون من شأنها أن تعزز أمن النظم العالمية للمعلومات والاتصالات السلوكية واللاسلكية وأن تساعد في مكافحة الإرهاب والإجرام المتصلين بالمعلومات؛ وطلبت إلى الأمين العام أن يقدم تقريرا في هذا الشأن إلى الجمعية العامة في دورتها الخامسة والخمسين.

٢ - وفي ١٤ آذار/مارس ٢٠٠٠، وجه الأمين العام مذكرة شفوية إلى الدول الأعضاء طالبا إليها موافاته بأرائها عملا بالدعوة الموجهة من الجمعية العامة. وتظهر الردود التي وردت من الحكومات حتى الآن في الفصل الثاني من هذا التقرير. وسوف تصدر أي ردود أخرى ترد لاحقا في إضافة لهذا التقرير.

ثانيا - الردود الواردة من الحكومات

الاتحاد الروسي

[الأصل: بالروسية]

[١٢ أيار/مايو ١٩٩٩]

مبادئ أمن المعلومات على الصعيد الدولي

المصطلحات المستخدمة

استخدمت لأغراض هذه المبادئ المصطلحات التالية:

١ - **مجال المعلومات:** وهو مجال النشاط الذي يشمل إنشاء المعلومات أو تحويلها أو استخدامها، بما في ذلك الوعي الفردي والاجتماعي والهيكلي الأساسي للمعلومات والاتصالات السلوكية واللاسلكية، والمعلومات نفسها.

- ٢ - **موارد المعلومات:** أي الهيكل الأساسي للمعلومات (المعدات والنظم اللازمة لإنشاء المعلومات وتجهيزها وتخزينها ونقلها)، بما في ذلك الخرائط النقطية (pit maps) وقواعد البيانات والمعلومات نفسها وتدفقات البيانات.
- ٣ - **حرب المعلومات:** المواجهة بين الدول في مجال المعلومات بهدف إتلاف نظم المعلومات وعملياتها ومواردها والهيكل الحيوية والنيل من النظم السياسية والاقتصادية والاجتماعية فضلا عن التأثير بصورة شاملة على الحالة النفسية عند السكان بغية زعزعة استقرار المجتمع والدولة.
- ٤ - **أسلحة المعلومات:** وهي السبل والوسائل المستخدمة بهدف إتلاف موارد المعلومات وعملياتها ونظمها في دولة ما، والتأثير سلبيا عن طريق المعلومات على النظم الدفاعية والإدارية والسياسية والاجتماعية والاقتصادية وغيرها من النظم الحيوية في هذه الدولة، فضلا عن التأثير بصورة شاملة على الحالة النفسية عند السكان بغية زعزعة استقرار المجتمع والدولة.
- ٥ - **أمن المعلومات:** وهي الحالة التي توجد فيها حماية للمصالح الأساسية للفرد والمجتمع والدولة في مجال المعلومات، بما في ذلك هيكل المعلومات والاتصالات السلكية واللاسلكية والمعلومات نفسها من حيث خصائصها، كالدقة والموضوعية والتوافر والسرية.
- ٦ - **الخطر الذي يهدد أمن المعلومات:** أي العوامل التي تعرض المصالح الأساسية للفرد والمجتمع والدولة للخطر في مجال المعلومات.
- ٧ - **أمن المعلومات على الصعيد الدولي:** وجود وضع في العلاقات الدولية يحول دون انتهاك الاستقرار العالمي وخلق خطر يهدد أمن الدول والمجتمع العالمي في مجال المعلومات.
- ٨ - **الاستخدام غير المشروع لنظم المعلومات والاتصالات السلكية واللاسلكية وموارد المعلومات:** أي استخدام نظم وموارد الاتصالات السلكية واللاسلكية والمعلومات دون التمتع بحق استخدامها أو على نحو يشكّل انتهاكا للقواعد أو التشريعات المعمول بها أو لقواعد القانون الدولي.
- ٩ - **التدخل غير المأذون به في نظم المعلومات والاتصالات السلكية واللاسلكية وموارد المعلومات:** أي التدخل في عمليات تجميع المعلومات أو تجهيزها أو تكديسها أو تخزينها أو عرضها أو استرجاعها أو نشرها أو استخدامها من أجل تعطيل السير العادي لنظم المعلومات أو للنيل من دقة موارد المعلومات أو سريتها أو إمكانية الوصول إليها.

١٠ - **الهيكل الحيوية:** وهي مرافق الدولة ونظمها ومؤسساتها التي يمكن أن يكون للتأثير المتعمد على موارد معلوماتها عواقب تؤثر مباشرة في الأمن الوطني (النقل، والإمداد بالكهرباء، والاستثمار والمال، والاتصالات، والهيئات الإدارية للدولة، ونظام الدفاع، وأجهزة إنفاذ القوانين، وموارد المعلومات الاستراتيجية، والمرافق العلمية والتطورات العلمية والتكنولوجية، والتجهيزات التي تنطوي على درجة عالية من المخاطر التكنولوجية أو الإيكولوجية، والهيئات المعنية بالتخفيف من حدة آثار الكوارث الطبيعية أو غيرها من حالات الطوارئ).

١١ - **الإرهاب الدولي المتصل بالمعلومات:** وهو استخدام نظم وموارد الاتصالات السلكية واللاسلكية والمعلومات وممارسة التأثير على هذه النظم أو الموارد في مجال المعلومات على الصعيد الدولي لأغراض إرهابية.

١٢ - **الجريمة الدولية المتصلة بالمعلومات:** وهي استخدام نظم وموارد الاتصالات السلكية واللاسلكية والمعلومات وممارسة التأثير على هذه النظم والموارد في مجال المعلومات على الصعيد الدولي لأغراض غير مشروعة.

المبدأ الأول

١ - يجب أن تكون أنشطة كل دولة وغيرها من الجهات الخاضعة للقانون الدولي في المجال الدولي للمعلومات عاملاً مساعداً على التنمية الاجتماعية والاقتصادية الشاملة ويجب الاضطلاع بها على نحو يتفق مع أهداف الحفاظ على الاستقرار والأمن العالميين، ومع حقوق السيادة للدول الأخرى، والمصالح الأمنية، ومبادئ تسوية المنازعات والصراعات بالوسائل السلمية، وعدم استخدام القوة، وعدم التدخل في الشؤون الداخلية، واحترام حقوق الإنسان وحرياته.

٢ - ويجب أن تتفق هذه الأنشطة أيضاً مع حق كل فرد في طلب المعلومات والأفكار وتلقيها ونشرها، وفقاً لما تنص عليه وثائق الأمم المتحدة ذات الصلة، على أن يوضع في الاعتبار أن من الجائز تقييد هذا الحق بالقانون من أجل حماية المصالح الأمنية لكل دولة.

٣ - وفي الوقت نفسه، يجب أن يكون لكل دولة وغيرها من الجهات الخاضعة للقانون الدولي حقوق متساوية لحماية موارد معلوماتها وهيكلها الحيوية من الاستخدام غير المشروع أو من التدخل غير المأذون به في المعلومات، وأن تتمكن من الاعتماد على الدعم من المجتمع الدولي في الحصول على هذه الحقوق.

المبدأ الثاني

على الدول أن تسعى إلى الحد من التهديدات في مجال أمن المعلومات على الصعيد الدولي وأن تمتنع لهذا الهدف عما يلي:

(أ) تطوير وإنشاء واستخدام وسائل للتأثير على موارد ونظم المعلومات أو إتلافها في دولة أخرى؛

(ب) الاستخدام المتعمد للمعلومات من أجل التأثير على الهياكل الحيوية لدولة أخرى؛

(ج) استخدام المعلومات للنيل من النظم السياسية والاقتصادية والاجتماعية في دول أخرى، أو للاضطلاع بحملة للتأثير على الحالة النفسية عند السكان من أجل زعزعة استقرار المجتمع؛

(د) التدخل غير المأذون به في نظم المعلومات والاتصالات السلكية واللاسلكية وموارد المعلومات، فضلا عن استخدامها بصورة غير قانونية؛

(هـ) التصرفات التي تميل إلى إنشاء سيادة أو سيطرة في مجال المعلومات؛

(و) منع الوصول إلى أحدث التكنولوجيات في مجال المعلومات وإيجاد أوضاع من التبعية التكنولوجية في مجال المعلومات مما يضر بدول أخرى؛

(ز) تشجيع أنشطة الرابطات والمنظمات والمجموعات الدولية الإرهابية أو المتطرفة أو الإجرامية أو أنشطة منتهكي القانون من الأفراد، التي تشكل خطرا على موارد المعلومات والهياكل الحيوية للدول؛

(ح) صياغة واعتماد خطط أو مبادئ تتوخى إمكانية شن حروب في مجال المعلومات وبإمكانها إثارة سباق في التسليح فضلا عن التسبب في توتر العلاقات بين الدول وتؤدي تحديدا إلى إثارة الحروب في مجال المعلومات؛

(ط) استخدام تكنولوجيات المعلومات وأدواتها بما يضر بحقوق الإنسان وحرياته الأساسية في مجال المعلومات؛

(ي) نشر المعلومات عبر الحدود على نحو يشكّل انتهاكا لمبادئ القانون الدولي وقواعده وللقوانين المحلية لبلدان معينة؛

(ك) التلاعب في تدفقات المعلومات وتشويه المعلومات وإخفاؤها من أجل إفساد البيئة النفسانية والروحية للمجتمع والقضاء على القيم التقليدية الثقافية والمعنوية والأخلاقية والجمالية؛

(ل) التوسع في مجال المعلومات وحيازة السيطرة على الهياكل الأساسية الوطنية للمعلومات والاتصالات السلوكية واللاسلكية في دولة أخرى، بما في ذلك شروط تشغيلها في المجال الدولي للمعلومات.

المبدأ الثالث

على الأمم المتحدة والوكالات ذات الصلة في منظومة الأمم المتحدة أن تعزز التعاون الدولي على الحد من التهديدات في مجال أمن المعلومات على الصعيد الدولي وإنشاء أساس قانوني دولي لهذا الغرض، من أجل:

- (أ) تحديد المعالم المميزة لحروب المعلومات وتصنيفها؛
- (ب) تحديد المعالم المميزة لأسلحة المعلومات وللأدوات التي يمكن اعتبارها أسلحة معلومات، وتصنيفها؛
- (ج) تقييد الاتجار بأسلحة المعلومات؛
- (د) حظر تطوير أسلحة المعلومات أو نشرها أو استخدامها؛
- (هـ) منع خطر نشوب حروب المعلومات؛
- (و) التسليم بأن خطر استعمال أسلحة المعلومات ضد الهياكل الحيوية يماثل التهديد باستخدام أسلحة الدمار الشامل؛
- (ز) تهيئة الأوضاع اللازمة للتبادل الدولي للمعلومات بصورة عادلة ومأمونة بالاستناد إلى قواعد ومبادئ القانون الدولي المعترف بها بوجه عام؛
- (ح) منع استخدام تكنولوجيات المعلومات وأدواتها لأغراض إرهابية أو أغراض إجرامية أخرى؛
- (ط) منع استخدام تكنولوجيات وأدوات المعلومات للتأثير على الوعي الاجتماعي من أجل زعزعة استقرار المجتمع والدولة؛
- (ي) وضع إجراء لتبادل المعلومات ومنع التأثير عبر الحدود غير المأذون به عن طريق المعلومات؛

- (ك) إنشاء نظام دولي للرصد من أجل تعقب التهديدات التي قد تنشأ في مجال المعلومات؛
- (ل) إنشاء آلية لرصد الامتثال لشروط النظام الدولي لأمن المعلومات؛
- (م) إنشاء آلية لتسوية حالات النزاع في مجال أمن المعلومات؛
- (ن) إنشاء نظام دولي لإصدار الشهادات المتعلقة بتكنولوجيات وأدوات المعلومات والاتصالات السلكية واللاسلكية (بما في ذلك البرامج والمعدات الالكترونية) بغية ضمان أمنها المعلوماتي؛
- (س) إقامة نظام للتعاون الدولي فيما بين أجهزة إنفاذ القوانين بغية منع الجريمة في مجال المعلومات وقمعها؛
- (ع) التنسيق على أساس طوعي بين القوانين الوطنية من أجل ضمان أمن المعلومات.

المبدأ الرابع

على الدول وغيرها من الجهات الخاضعة للقانون الدولي أن تأخذ على عاتقها المسؤولية الدولية عن الأنشطة التي تضطلع بها في مجال المعلومات، سواء في نطاق ولايتها القضائية أو تحت رعاية منظمات دولية تنتمي إلى عضويتها، وعن امتثال أي من هذه الأنشطة للمبادئ المنصوص عليها في هذه الوثيقة.

المبدأ الخامس

كل منازعة بين الدول أو غيرها من الجهات الخاضعة للقانون الدولي قد تنشأ عن تطبيق هذه المبادئ تُسوى باستخدام الإجراءات المرعية لتسوية المنازعات بالوسائل السلمية.

الأردن

[الأصل: بالعربية]

[١٦ أيار/مايو ١٩٩٩]

١ - إن استخدام التكنولوجيا ووسائل المعلومات لهما نتائج إيجابية على المجتمع الدولي في مجال صون الاستقرار والأمن ولكن إذا أسيء استخدام هذه التطورات والتقنيات الحديثة فإنها ستؤدي إلى:

- (أ) سهولة تنظيم شبكات إرهابية لتوزع عناصرها على مساحات جغرافية واسعة جدا نظرا لإمكانيات الاتصالات السريعة؛
- (ب) صعوبة رصد الاتصالات الحديثة نظرا للتعقيدات التكنولوجية المتسارعة والمتطورة ونظرا لوجود قوانين في معظم الدول تحد من التدخل في حرية الأفراد في الاتصالات.
- ٢ - حرصا منا على اتخاذ الإجراءات المناسبة وتحسبا لوقوع أي عمل إرهابي فإننا نوصي بما يلي:
- (أ) وضع أو استحداث (قانون طوارئ خاص) يسمح للأجهزة الأمنية بالدخول أو السيطرة جزئيا على مراكز سيطرة الشركات التي تتعامل مع الأنظمة المتطورة؛
- (ب) التنسيق مع الشركات والمؤسسات التي تعنى بالاتصالات للسماح بتدريب وتأهيل مختصين من الجهات الأمنية للتعامل مع هذه الأنظمة عند حدوث أزمات؛
- (ج) دعم قطاع تكنولوجيا المعلومات والاتصالات ومفاهيم الأمن المتعلقة بها وتوفير البنية التحتية والتدريب المناسب لكي تساعد في حفظ الأمن والسلام الدوليين.

قطر

[الأصل: بالعربية]

[١٧ أيار/مايو ١٩٩٩]

- ١ - **التجسس:** مقاومة اطلاع طرف غير مصرح له على محتويات أنظمة المعلومات والاتصالات الدولية.
- ٢ - **التخريب:** مقاومة التخريب الجزئي أو الكلي لأنظمة المعلومات والاتصالات الدولية.
- ٣ - **التوثيق:** توثيق المعلومات المرسله عبر أنظمة المعلومات والاتصالات ومنها الملكية الفكرية.
- ٤ - **التزوير:** مقاومة تزوير المعلومات المرسله عبر أنظمة المعلومات والاتصالات الدولية.
- ٥ - **الحماية:** تطوير الحماية الالكترونية للمعلومات المرسله عبر أنظمة المعلومات والاتصالات الدولية.
- ٦ - **التشريع:** وضع القوانين اللازمة لجميع التعاملات الالكترونية التي تضمن حقوق المتعاملين ومعاقبة المخالفين لهذه القوانين.