Generalversammlung

Verteilung: Allgemein
30. Januar 2004

Achtundfünfzigste Tagung
Tagesordnungspunkt 91 *b*)

Resolution der Generalversammlung

[*auf Grund des Berichts des Zweiten Ausschusses (A/58/481/Add.2)*]

58/199. Schaffung einer globalen Kultur der Cyber-Sicherheit und Schutz kritischer Informationsinfrastrukturen

Die Generalversammlung,

unter Hinweis auf ihre Resolutionen 57/239 vom 20. Dezember 2002 über die Schaffung einer globalen Kultur der Cyber-Sicherheit, 55/63 vom 4. Dezember 2000 und 56/121 vom 19. Dezember 2001 über die Schaffung der Rechtsgrundlage für die Bekämpfung des kriminellen Missbrauchs von Informationstechnologien sowie 53/70 vom 4. Dezember 1998, 54/49 vom 1. Dezember 1999, 55/28 vom 20. November 2000, 56/19 vom 29. November 2001 und 57/53 vom 22. November 2002 über Entwicklungen auf dem Gebiet der Informationstechnik und der Telekommunikation im Kontext der internationalen Sicherheit,

in Anerkennung dessen, dass Regierungen, Wirtschaftsunternehmen, andere Organisationen und individuelle Nutzer den Informationstechnologien immer größere Bedeutung beimessen, wenn es darum geht, die sozioökonomische Entwicklung zu fördern, wesentliche Güter und Dienstleistungen bereitzustellen, Geschäfte abzuwickeln und Informationen auszutauschen,

im Hinblick auf die zunehmende Verknüpfung der kritischen Informationsinfrastrukturen der meisten Länder – wie beispielsweise derjenigen, die unter anderem zur Energieerzeugung, -übertragung und -verteilung, für den Luft- und Seetransport, im Bank- und Finanzdienstleistungssektor, im elektronischen Geschäftsverkehr, zur Wasser- und Nahrungsmittelversorgung und auf dem Gebiet der öffentlichen Gesundheit eingesetzt werden – sowie der kritischen Informationsinfrastrukturen, die deren Tätigkeiten in immer stärkerem Maße verbinden und sich darauf auswirken,

in der Erkenntnis, dass jedes Land seine eigenen kritischen Informationsinfrastrukturen festlegen wird,

sowie in der Erkenntnis, dass diese zunehmende technologische Interdependenz auf einem komplexen Netzwerk von kritischen Informationsinfrastruktur-Komponenten beruht,

feststellend, dass die kritischen Informationsinfrastrukturen heute auf Grund der zunehmenden Vernetzung einer größeren Zahl und Vielfalt von Bedrohungen ausgesetzt sind und mehr Angriffsflächen bieten, wodurch neue Sicherheitsprobleme entstehen,

sowie feststellend, dass es für den wirksamen Schutz kritischer Informationsinfrastrukturen unter anderem notwendig ist, die Bedrohungen aufzuzeigen und die Anfälligkeit zu vermindern, denen die kritischen Informationsinfrastrukturen ausgesetzt sind, die Schäden und die Ausfallzeit im Falle eines Schadens oder eines Angriffs auf ein Mindestmaß zu beschränken und die Schadensursache oder den Urheber eines Angriffs zu ermitteln,

in der Erkenntnis, dass ein wirksamer Schutz die Kommunikation und Zusammenarbeit aller Interessengruppen auf nationaler und internationaler Ebene erfordert und dass die einzelstaatlichen Anstrengungen durch wirksame fachliche Zusammenarbeit der Interessengruppen auf internationaler und regionaler Ebene unterstützt werden sollen,

sowie in der Erkenntnis, dass die Wirksamkeit der Zusammenarbeit bei der Bekämpfung des kriminellen Missbrauchs von Informationstechnologien und bei der Schaffung einer globalen Kultur der Cyber-Sicherheit durch Lücken beim Zugang der Staaten zu den Informationstechnologien und bei ihrer Nutzung herabgesetzt werden kann, und feststellend, dass der Transfer von Informationstechnologien, insbesondere in die Entwicklungsländer, erleichtert werden muss,

ferner in der Erkenntnis, wie wichtig die internationale Zusammenarbeit für die Herbeiführung der Cyber-Sicherheit und den Schutz kritischer Informationsinfrastrukturen ist, in deren Rahmen die einzelstaatlichen Anstrengungen zur Steigerung der personellen Kapazitäten und der Lern- und Beschäftigungsmöglichkeiten, zur Verbesserung der öffentlichen Dienstleistungen und zur Steigerung der Lebensqualität durch den Einsatz hochentwickelter, zuverlässiger und sicherer Informations- und Kommunikationstechnologien und -netze und die Förderung des allgemeinen Zugangs unterstützt werden,

feststellend, dass die zuständigen internationalen und regionalen Organisationen darauf hinarbeiten, die Sicherheit der kritischen Informationsinfrastrukturen zu erhöhen,

in der Erkenntnis, dass es gilt, kritische Informationsinfrastrukturen unter gebührender Berücksichtigung der anwendbaren innerstaatlichen Datenschutzvorschriften und anderer einschlägiger Rechtsvorschriften zu schützen,

1. *nimmt Kenntnis* von den in der Anlage dieser Resolution enthaltenen Elementen für den Schutz kritischer Informationsinfrastrukturen;

2. *bittet* alle zuständigen internationalen Organisationen, namentlich die zuständigen Organe der Vereinten Nationen, diese Elemente für den Schutz kritischer Informationsinfrastrukturen bei allen künftigen Tätigkeiten auf dem Gebiet der Cyber-Sicherheit oder des Schutzes kritischer Informationsinfrastrukturen nach Bedarf in Betracht zu ziehen;

3. *bittet* die Mitgliedstaaten, unter anderem diese Elemente in Betracht zu ziehen, wenn sie Strategien zur Verminderung der Risiken für kritische Informationsinfrastrukturen im Einklang mit den innerstaatlichen Rechts- und sonstigen Vorschriften entwickeln;

4. *bittet* die Mitgliedstaaten und alle zuständigen internationalen Organisationen, bei ihren Vorbereitungen für die zweite Phase des Weltgipfels über die Informationsgesellschaft, die vom 16. bis 18. November 2005 in Tunis stattfinden soll, unter anderem diese Elemente sowie die Notwendigkeit des Schutzes kritischer Informationsinfrastrukturen in Betracht zu ziehen;

5. *ermutigt* diejenigen Mitgliedstaaten und zuständigen regionalen und internationalen Organisationen, die Strategien für die Cyber-Sicherheit und den Schutz kritischer Informationsinfrastrukturen entwickelt haben, ihre besten Verfahrensweisen und

Maßnahmen weiterzugeben, die anderen Mitgliedstaaten bei ihren Bemühungen um die Förderung der Cyber-Sicherheit behilflich sein könnten;

6. *unterstreicht*, dass verstärkte Anstrengungen unternommen werden müssen, um die digitale Kluft zu überbrücken, den universellen Zugang zu Informations- und Kommunikationstechnologien zu ermöglichen und kritische Informationsinfrastrukturen zu schützen, indem der Transfer von Informationstechnologien, insbesondere in die Entwicklungsländer, vor allem in die am wenigsten entwickelten Länder, und der Aufbau von Kapazitäten in diesen Ländern erleichtert wird, damit sich alle Staaten bei ihrer sozioökonomischen Entwicklung die Informations- und Kommunikationstechnologien voll zunutze machen können.

78. Plenarsitzung
23. Dezember 2003

Anlage

Elemente für den Schutz kritischer Informationsinfrastrukturen

1. Einrichtung von Netzen zur Notfallwarnung im Fall von Schwachstellen, Bedrohungen und Problemen der Cyber-Sicherheit.

2. Erhöhung des Problembewusstseins, um den Interessengruppen das Verständnis der Beschaffenheit und des Umfangs ihrer kritischen Informationsinfrastrukturen sowie der Rolle zu erleichtern, die ihnen beim Schutz dieser Informationsinfrastrukturen jeweils zukommt.

3. Prüfung der Infrastrukturen und Feststellung eventueller Interdependenzen, wodurch der Schutz dieser Infrastrukturen verbessert wird.

4. Förderung von Partnerschaften zwischen öffentlichen wie privaten Interessengruppen, mit dem Ziel, Informationen über kritische Informationsinfrastrukturen auszutauschen und zu analysieren und so Beschädigungen dieser Infrastrukturen oder Angriffe auf sie zu verhindern, zu untersuchen und Gegenmaßnahmen zu ergreifen.

5. Schaffung und Unterhaltung von Kommunikationsnetzen für den Krisenfall sowie deren Erprobung, mit dem Ziel, ihre Sicherheit und Stabilität in Notfällen zu gewährleisten.

6. Gewährleistung dessen, dass Politiken, die die Verfügbarkeit von Daten betreffen, der Notwendigkeit des Schutzes von kritischen Informationsinfrastrukturen Rechnung tragen.

7. Erleichterung der Rückverfolgung von Angriffen auf kritische Informationsinfrastrukturen und gegebenenfalls Offenlegung der diesbezüglichen Informationen an andere Staaten.

8. Abhaltung von Ausbildungskursen und Übungen zur Verbesserung der Antwortkapazität und Erprobung von Kontinuitäts- und Eventualfallplänen im Falle eines Angriffs auf die Informationsinfrastrukturen und Ermutigung von Interessengruppen, ähnliche Tätigkeiten durchzuführen.

9. Gewährleistung angemessener materiellrechtlicher und verfahrensrechtlicher Vorschriften und Bereitstellung von ausgebildetem Personal, damit die Staaten Angriffe auf kritische Informationsinfrastrukturen untersuchen und strafrechtlich verfolgen und diese Untersuchungen gegebenenfalls mit anderen Staaten koordinieren können.

10. Gegebenenfalls Zusammenarbeit auf internationaler Ebene, um kritische Informationsinfrastrukturen zu schützen, namentlich durch die Entwicklung und Koordinierung von Notfallwarnsystemen, die Weitergabe und Analyse von Informationen über Schwachstellen, Bedrohungen und Zwischenfälle und die Koordinierung von Untersuchungen von Angriffen auf diese Infrastrukturen im Einklang mit den innerstaatlichen Rechtsvorschriften.

11. Förderung der nationalen und internationalen Forschung und Entwicklung sowie der Anwendung von den internationalen Normen entsprechenden Sicherheitstechnologien.