Bekämpfung von „Cybercrime“: Forderungen des UN-Weltgipfels der Informationsgesellschaft

Irini E. Vassilaki

Kanzlei Jones Day
Prinzregentenstrasse 1, D – 80538 München
ivassilaki@jonesday.com

Schlagworte: Cyber-Kriminalität, Cybercrime, Cyber-Sicherheit, UN-Weltgipfel der Informationsgesellschaft, Sicherheitsmanagement, Informationsteilhabe

Abstract: Der Beitrag stellt dar, welches Konzept der UN-Weltgipfel der Informationsgesellschaft zum Thema „Cyber-Kriminalität“ ausgearbeitet hat, nämlich die Vorschläge der Vertreter der internationalen Gemeinschaft, mittels welcher Mechanismen diese Vorschläge umgesetzt werden sollen.

1. Einleitung

Der Weltgipfel zur Informationsgesellschaft (WSIS) war eine von den Vereinten Nationen organisierte Konferenz zu den Themen Information und Kommunikation. Er wurde von der Internationalen Fernmeldeunion (International Telecommunication Union – ITU), einer Teilorganisation der UNO, in zwei Teilen veranstaltet. Der erste Teil fand vom 10. bis 12. Dezember 2003 in Genf statt, wo zwei Dokumente verabschiedet wurden:

- Die Genfer Prinzipienerklärung (Geneva Declaration of Principles),
- Der Genfer Aktionsplan (Geneva Plan of Action).

Der zweite Teil fand vom 16. bis 18. November 2005 in Tunis statt. Hier wurden die Dokumente des ersten Teils bestätigt und zwei weitere Erklärungen verabschiedet:

- Die Tunis Verpflichtung (Tunis Commitment) und
- Die Tunis Agenda für die Informationsgesellschaft (Tunis Agenda for the Information Society).

Ein wesentlicher Problembereich des Weltgipfels war die Prävention und Bekämpfung der Cyber-Kriminalität. Im Folgenden werde ich darstellen, welches Konzept der Weltgipfel zu diesem Thema ausgearbeitet hat, nämlich die Vorschläge, die die Vertreter der internationalen Gemeinschaft gemacht haben

und mittels welcher Mechanismen diese Vorschläge umgesetzt werden sollen. Dafür werde ich Dokumente verwenden, die im Weltgipfel verabschiedet wurden und die Resolutionen der Generalversammlung der Vereinigten Nationen, auf die die Dokumente verweisen.

2. Rahmen der Bekämpfung der Cyber-Kriminalität

2.1. Ausgangspunkt: “Cyber-Sicherheit”

Sowohl der Genfer Aktionsplan als auch die Tunis Agenda betonen, dass die Schaffung von Vertrauen und Sicherheit beim Einsatz von Informations- und Kommunikationstechnologien zu den wichtigsten Stützen der Informationsgesellschaft gehört. Sie unterstreichen die Notwendigkeit, dass alle Teilnehmer der Informationsgesellschaft wie zB Regierungen, privatwirtschaftliche Unternehmen oder individuelle Nutzer eine globale Kultur der “Cyber-Sicherheit” entwickeln und implementieren sollen. Die globale Kultur der Cyber-Sicherheit erfordert – nach der Resolution 57/239 der Generalversammlung – von allen Teilnehmern der Informationsgesellschaft die Beachtung folgender, einander ergänzender Bausteine:

- Problembewusstsein
- Verantwortungsbewusstsein
- Antwortmaßnahmen
- Ethische Fragen
- Demokratie
- Risikobewertung
- Gestaltung und Durchführung von Sicherheitsmaßnahmen
- Sicherheitsmanagement
- Neubewertung

2.2. Grundlagen

Das Vertrauen beim Einsatz von IT-Technologien wird durch den Missbrauch derselbigen erheblich beeinträchtigt. Der Genfer Aktionsplan und die Tunis Agenda betonen in diesem Zusammenhang die Bedeutung der Strafverfolgung von Cyber-Kriminalität. Was unter dem Begriff “Cybercrime” zu verstehen ist, wird in den Texten nicht erläutert. Es wird lediglich darauf hingewiesen, dass bestehende und potenzielle Gefahren für Informations- und Kommunikationstechnologien geprüft und im Zusammenhang mit der Informations- und Netzwerksicherheit behandelt werden sollen. Gleichwohl werden bestimmte Themen hervorgehoben, die besonders berücksichtigt werden sollen. Der Genfer Aktionsplan verlangt Präventivmaßnahmen gegen

missbräuchliche IT-Anwendungen, die Rassismus, Rassendiskriminierung, Fremdenfeindlichkeit, Kindesmissbrauch, einschließlich Pädophile und Kinderpornographie sowie Menschenhandel und Ausbeutung von Menschen fördern. Darüber hinaus wird Aufklärung der Nutzer gefordert, um das Bewusstsein über die Rechtswidrigkeit der Online-Piraterie und der Verletzung der Persönlichkeit zu stärken. Überdies wird Spam als Gefahr erwähnt, die bekämpft werden soll. Besondere Bedeutung ist der Tatsache beizumessen, dass bei der Tunis Verpflichtung die Prävention des Missbrauchs der IT-Technologien gefordert wird, die für terroristische Zwecke eingesetzt werden.

Der Weltgipfel hat deutlich die Grenzen bezeichnet, innerhalb derer die Cyber-Kriminalität bekämpft werden soll. Die Tunis Verpflichtung bestätigt das Ziel des Weltgipfels, zur Entwicklung einer Informationsgesellschaft beizutragen, die menschenorientiert ist und in der die Menschenwürde geachtet wird. Dafür stellt das Recht auf "Informationsteilhabe" eine unabdingbare Voraussetzung dar. Alle Menschen auf der Welt sollen die Gelegenheit haben, an der Informationsgesellschaft teilzunehmen, und niemandem sollten die Vorteile verwehrt sein. In diesem Zusammenhang sind Meinungs- und Informationsfreiheit wichtig, denn durch sie kann sichergestellt werden, dass ohne Rücksicht auf Grenzen Informationen und Gedankengut gesucht, empfangen und verbreitet wird. Damit wird Kommunikation als grundlegender sozialer Prozess gewährleistet. Weil diese die Grundlage aller sozialen Organisation darstellt, ist sie – wie die Genfer Erklärung betont – Dreh- und Angelpunkt der Informationsgesellschaft.

Unter diesem Gesichtspunkt muss die Prävention des Missbrauchs von Informationstechnologien im Rahmen der Gewährleistung von Grundrechten realisiert werden. Wichtig ist insbesondere, dass die Rechte auf Privatsphäre und freie Meinungsäußerung respektiert und geschützt werden, wie es in der Charta der Vereinten Nationen und in der Allgemeinen Erklärung der Menschenrechte verankert ist.

2.3 Implementierungsmechanismen

Im Rahmen der WSIS wurde festgelegt, dass bei der Bekämpfung der Cyber-Kriminalität Regierungen, der Privatsektor, die Zivilgesellschaft, die Vereinten Nationen und andere internationale Organisationen kooperieren sollen. Dabei sollen die unterschiedlichen Rollen, die Verantwortlichkeit als auch die Expertise der Mitwirkenden berücksichtigt werden.

Zunächst sollen Gesetze verabschiedet werden, die die Untersuchung und Verfolgung dieser Missbräuche gestatten, wirksamen Beistand auf Behördenebene fördern und die institutionelle Unterstützung auf internationaler Ebene verstärken. Dazu sollen Rechtshilferegelungen erlassen werden, um die rechtmäßige und schnelle Sammlung von Beweismaterial und dessen Austausch si-

cherzustellen. Neben dem gesetzlichen Rahmen wird von dem Privatsektor die Entwicklung selbstregulatorischer Maßnahmen, die Ausarbeitung von “Codes of Conduct” und anderer effektiver Strategien erwartet, die gegen den Missbrauch der IT-Technologien, insbesondere dem Schutz von Kindern und Jugendlichen, dienen.

Für den erfolgreichen Einsatz technischer Maßnahmen, die den Missbrauch der IT-Technologien erschweren, sollen bewährte Vorgehensweisen und Erfahrungen auf dem Gebiet der Informations- und Netzsicherheit ausgetauscht und ihr Einsatz durch alle Betroffenen gefördert werden. Interessierte Länder sollen Koordinierungsstellen für die Echtheit-Behandlung und -Bewältigung von Sicherheitsvorfällen einrichten und ein Kooperationsnetz zur Bewältigung solcher Vorfälle schaffen.

WSIS betont, dass Initiativen und Richtlinien, die Vertrauen und Sicherheit im IT-Bereich fördern sollen, auch das Recht auf Privatsphäre sowie den Daten- und Verbraucherschutz beachten sollen.

Um die Cyber-Kriminalität wirksam zu bekämpfen, wird eine geeignete Ausbildung und Ausrüstung der Strafverfolgungsbehörden verlangt.

Last but not least werden Maßnahmen erwartet, die der Aufklärung der Nutzer dienen und ihr Bewusstsein für bestehende und potenzielle Gefahren der IT-Technologien sensibilisieren sollen. Die Öffentlichkeit soll auf die Notwendigkeit hingewiesen werden, den kriminellen Missbrauch der IT-Technologien zu verhüten und zu bekämpfen.

Der Weltgipfel lädt außerdem akademische Kreise ein, Forschungsarbeiten über die ethischen Dimensionen der Informations- und Kommunikationstechnologien und deren Missbrauch durchzuführen.

3. Ergebnisse

Strategisch richtig ist die Entscheidung des Weltgipfels, keine detaillierten Aussagen über Umfang und Erscheinungsformen der Cyber-Kriminalität zu machen. Weil diese im Wandel steht, ermöglicht der Verzicht auf eine dogmatische Beschreibung des Phänomens die Anwendung des entsprechenden Aktionsplans auch auf Kriminalitätsformen, die heute noch nicht in den Bereich der Cyber-Kriminalität fallen, weil keine zuverlässigen Informationen vorhanden sind.

Alles in allem hat es der Weltgipfel geschafft, unterschiedliche Interessen auf rechtsstaatliche Weise zu balancieren und sich mit den wichtigen Problemen zu befassen. Es liegt nunmehr an der internationalen Gemeinschaft, die in Genf und Tunis ausgearbeiteten Impulse aufzugreifen, und daraus eine umfassende Strategie zu entwickeln und umzusetzen, die sowohl Prävention als auch Bestrafung der Cyber-Kriminalität erreichen wird.