XXIV.GP.-NR
7525 /AB
-4. April 2011

zu 7593 /J

BM.I REPUBLIK ÖSTERREICH
BUNDESMINISTERIN FÜR INNERES

Frau
Präsidentin des Nationalrates
Mag. Barbara Prammer
Parlament
1017 Wien

DR. MARIA FEKTER
HERRENGASSE 7
1014 WIEN
POSTFACH 100
TEL +43-1 53126-2352
FAX +43-1 53126-2191
ministerbuero@bmi.gv.at

GZ BMI-LR2220/0186-II/BK/4.3/201111

Wien, am 1. April 2011

Der Abgeordnete zum Nationalrat Mag. Johann Maier, Genossinnen und Genossen haben am 4. Februar 2011 unter der Zahl 7593/J an mich eine schriftliche parlamentarische Anfrage betreffend „Internetkriminalität – Strafdelikte durch IT-Medium im Jahr 2010" gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zu Frage 1:

Im Jahr 2010 wurden insgesamt 201 Fälle von Tatbegehungen mittels IT-Mediums angezeigt.

Mit 01.01.2010 wurden die kriminologischen Sachverhalte in der Kriminalstatistik geändert. Diese setzen sich nun wie folgt zusammen:

Denial of Service Attack:	Tatobjekt ist das IT-Medium (Hardware-Sabotage)
Abhören von Datenverkehr mittels IT-Medium:	Tatbegehung mittels IT-Medium (Abhören von Datenverkehr)
Hacking:	Tatobjekt ist das IT-Medium (Hacking)
Einsatz von Schadsoftware:	Tatobjekt ist das IT-Medium (Software-Sabotage) Tatobjekt ist das IT-Medium (Logische Bomben) Tatobjekt ist das IT-Medium (Trojanische Pferde) Tatobjekt ist das IT-Medium (Viren) Tatobjekt ist das IT-Medium (Würmer)

Phreaking:	Tatobjekt ist das IT-Medium (Telefon-Phreaking

Zu Frage 2:

5.

Zu Frage 3:

Die kriminologischen Sachverhalte „Tatbegehung mittels IT-Medium" und „Tatobjekt ist das IT-Medium (Datenbezogene Wirtschaftsspionage)" werden in der Kriminalstatistik nicht mehr ausgewertet.

Zu Frage 4:

2 Fälle von „Denial of Service Attack".

Zu Frage 5:

142.

Zu den Fragen 6 bis 9:

Im Jahr 2010 wurden 39 Fälle von „Einsatz von Schadsoftware" angezeigt. Unter diesen kriminologischen Sachverhalt fallen „Trojanische Pferde", „Viren", „Sabotage Software" und „Würmer".

Zu Frage 10:

13.

Zu den Fragen 11 bis 19:

Angezeigte Fälle	Jahr 2010
Widerrechtlicher Zugriff auf ein Computersystem - § 118a StGB	79
Verletzung des Telekommunikationsgeheimnisses - § 119 StGB	8
Missbräuchliches Abfangen von Daten - § 119a StGB	9
Datenbeschädigung - § 126a StGB - Vergehen	81
Datenbeschädigung - § 126a StGB - Verbrechen	4
Störung der Funktionsfähigkeit eines Computersystems - § 126b StGB	25
Missbrauch von Computerprogrammen oder Zugangsdaten - § 126c StGB	78
Betrügerischer Datenverarbeitungsmissbrauch - § 148a StGB - Vergehen	127
Betrügerischer Datenverarbeitungsmissbrauch - § 148a StGB - Verbrechen	32

Die jeweiligen Zusatzfragen zu den Entwicklungen im Jahr 2011 können aufgrund des noch fehlenden Datenbestandes nicht beantwortet werden.

Zu Frage 20:

Auf europäischer Ebene bestehen derzeit mit den Richtlinien zum Datenschutz, zum Fernabsatz, zum E-Commerce, über die Vorratsdatenspeicherung sowie dem EU-Rahmenbeschluss über Angriffe auf Informationssysteme, sehr umfangreiche und für die Bekämpfung der Internetkriminalität ausreichende Regelungen. Überdies wird auf europäischer Ebene an einer neuen Richtlinie über Angriffe auf Informationssysteme gearbeitet, welche die Bekämpfung von BotNetzen erleichtern soll.

Zu Frage 21:

1874.

Zu Frage 22:

Derzeit wird mit den strafrechtlichen Tatbeständen für die Bekämpfung der Internetkriminalität das Auslangen gefunden.

Zu Frage 23:

Die Kriminalstatistik zeigt, dass vor allem bei den Betrugsformen durch Missbrauch des Internets, wie beispielsweise mit gefakten Webshops sowie im Bereich des Hackings und beim Einsatz von Schadsoftware ein starker Anstieg festzustellen ist. Strafrechtlich geht es hier vor allem um die Verletzung der Privatsphäre und bestimmter Berufsgeheimnisse sowie um strafbare Handlungen gegen fremdes Vermögen.

Zu Frage 24:

Die internationale Zusammenarbeit zwischen den Sicherheitsbehörden erfolgt entweder im Interpolweg oder über Europol, wodurch eine rasche Bearbeitung der Anfragen und Informationen gesichert ist. Darüber hinaus verstärken und unterstützen internationale Aktivitäten und Initiativen die Zusammenarbeit der zuständigen Sicherheitsbehörden durch Schaffung von Plattformen für einen unmittelbaren Informationsaustausch. Die Erfolge bei der Bekämpfung dieser Kriminalitätsform zeigen, dass die Zusammenarbeit grundsätzlich sehr gut funktioniert.