Faktenblatt: Kabelaufklärung

Digitale Gesellschaft, CH-4000 Basel
www.digitale-gesellschaft.ch

Mit der Kabelaufklärung will der Nachrichtendienst des Bundes die Telekommunikationsverbindungen, welche von der Schweiz ins Ausland führen, nach definierten Stichworten durchsuchen. Da die meiste Internetkommunikation der Schweizer Bevölkerung über ausländische Server und Netzwerke führt, sind wir alle von dieser Massenüberwachung betroffen.

Wie wird dies konkret umgesetzt?

Das neue Nachrichtendienstgesetz sieht vor, dass «Betreiberinnen von leitungsgebundenen Netzen» (Provider) verpflichtet sind, die entsprechenden Datensignale an das Zentrum für elektronische Operationen ZEO der Armee zu liefern.

Dieser «durchführende Dienst» durchsucht die Datenströme nach Stichworten und leitet die gewonnenen Informationen, die auf eine Bedrohung der inneren Sicherheit hinweisen, an den Nachrichtendienst des Bundes weiter.

Welche Einschränkungen gibt es (z.B. auf ausländischen Datenverkehr)?

Sobald sich der Sender *oder* Empfänger im Ausland befindet (in den Erläuterungen zum Gesetzesentwurf wird von IP-Adressen gesprochen), darf die Kommunikation überwacht werden. Bei Datenleitungen, welche die Landesgrenzen überschreiten, ist diese Voraussetzung automatisch erfüllt.

Wie wirkt das mehrstufige Bewilligungsverfahren?

Ein Überwachungsantrag enthält Angaben zur «Notwendigkeit des Einsatzes», «die Kategorien von Suchbegriffen» (nach denen die Kommunikation durchsucht werden soll), eine Auflistung der betroffenen Provider, sowie Beginn und Ende des Auftrags.

2003 untersuchte die Geschäftsprüfungsdelegation der Eidgenössischen Räte das bereits bestehende Satellitenaufklärungssystem «Onyx»: Zu diesem Zeitpunkt durchsuchte die Überwachungsanlage auf der Basis von rund dreissig Aufträgen nach je zwischen fünf und mehreren hundert Schlüsselwörtern.

Das System darf also nicht als gezielten, temporären Eingriff verstanden werden. Vielmehr werden immer Aufträge bestehen, die möglichst sämtliche E-Mails, Suchanfragen, Zugänge zu Webforen, die Internettelefonie etc. nach den definierten Suchkriterien überwachen und gegebenenfalls anschlagen. Um umfassend zu sein, werden sämtliche grösseren Provider von der «Ausleitung» der Daten betroffen sein.

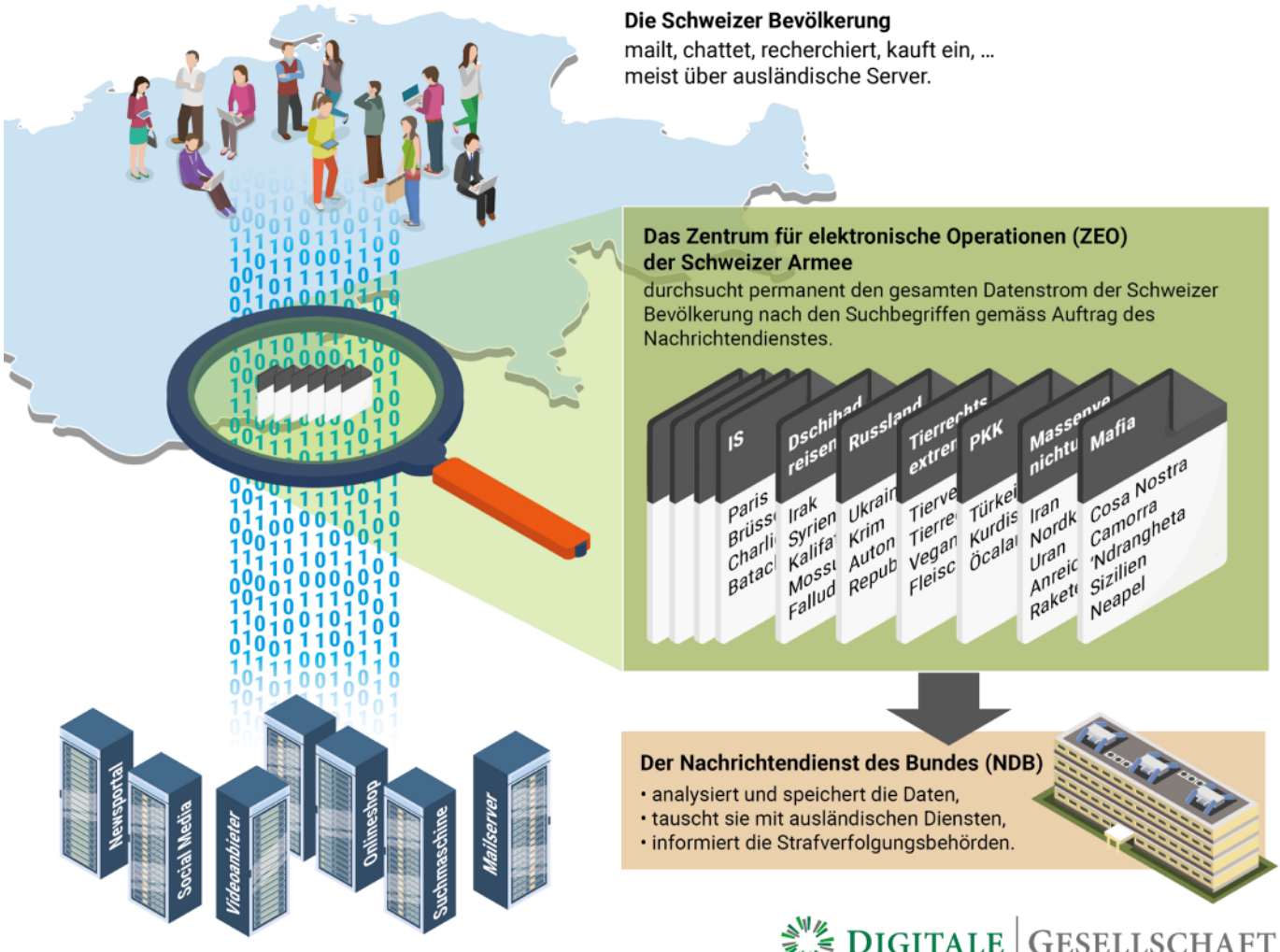
Was sich über die Zeit durch das Bewilligungsverfahren ändert, sind die Suchkategorien, die betroffenen Anbieterinnen und die überwachten Internetkommunikationsarten. Aber nicht die Massenüberwachung an sich.

Wenn die Dienstbetreiber den Datenaustausch verschlüsseln, ist dann die Privatsphäre und das Fernmeldegeheimnis wieder gewahrt?

Das Gesetz betrifft neben den Providern zusätzlich auch - nicht konkreter definierte - «Anbieterinnen von Telekommunikationsdienstleistungen».

Damit können einerseits Anbieterinnen von Festnetz- & Mobilfunknetzen, Internettelefonie, Internetzugängen und anderen Informationsnetzen gemeint sein. Aber auch Betreiberinnen von E-Mail-Infrastruktur, Webforen oder Kurznachrichtendiensten. Von ihnen angebrachte (Transport-)Verschlüsselung müssen vor der Weiterleitung der Daten an das ZEO entfernen werden.

Tatsächlich schützt nur eine konsequente und sichere Ende-zu-Ende-Verschlüsselung vor der Massenüberwachung.



DIGITALE | GESELLSCHAFT