



**W**ir stehen an der Schwelle des Übergangs der Industrie- und Dienstleistungsgesellschaft in die Informations- oder Digitalgesellschaft. Dabei sind die Begriffe Globalisierung und Internet zu eigentlichen Sinnbildern der neuen, revolutionären Möglichkeiten des Wirtschaftens geworden. Eine ähnliche Euphorie muss wohl auch zu Beginn der Industriegesellschaft bei der Einführung der Dampfmaschine geherrscht haben. Der damalige technische Machbarkeitswahn ist für uns heute unverständlich geworden. Doch auch wir würden einer Selbsttäuschung unterliegen, wenn wir nur die Chancen, nicht aber die Risiken der neuen technischen Möglichkeiten diskutieren würden.

**Eldorado für Wirtschaftskriminelle**

Die Aufsehen erregenden Ereignisse, welche zurzeit von Hackern verursacht werden, überschatten dabei die Tatsache, dass auch Wirtschaftskriminelle zunehmend ihr Unwesen im Internet treiben. Kaum jemand spricht darüber, wie viele Anlagebetrüger, gezinkte Spielcasinos, Kreditkartendiebe und weitere Wirtschaftskriminelle sich bereits heute erfolgreich im Internet bewegen.

Ganz selten wird ein Fall aus diesem Bereich öffentlich diskutiert. So zum Beispiel letztes Jahr, als ein Anbieter einer Pornoseite in den USA überführt wurde. Ihm war es gelungen, von einer Million Kreditkarten durchschnittlich 50 US-Dollar widerrechtlich abzubuchen und ins Ausland zu transferieren (der so genannte Fall «Netfill»). Pikanterweise flog die Sache nicht dadurch auf, dass diese Transaktionsvolumina seiner Hausbank irgendwie ungewöhnlich vorgekommen wären, sondern weil der Kreditkarten-Firma Visa auffiel, wie häufig Kunden Falschbelastungen durch diese Firma reklamierten.

Natürlich ist ein Schaden in Höhe von 50 Millionen US-Dollar nicht vergleichbar mit den Milliarden Schäden eines «I love you»-Virus. Dennoch ist höchst beunruhigend, welchen kriminellen Erfolg der sehr einfach konstruierte Netfill-Betrug dank des Internet erzielte. Wenn schon ein unbedarfter Einzeltäter dank der hohen Anonymität und Effizienz des globalen Internets einen derartigen Erfolg erzielen kann, dann mag man sich nicht ausmalen, wie erfolgreich organisierte Kriminalität im Internet sein kann.

**Fehlende Fallbeispiele**

Doch wo bleiben die wirklich grossen Fälle von Wirtschaftskriminalität im Internet? Es gibt kaum bekannte Beispiele. Teilweise ziehen daher die Strafverfol-

**Das Computervirus «I love you» zeigt die Kehrseite der globalen Vernetzung – ebenso grosse Gefahr droht von organisierten Wirtschaftskriminellen**

Von Christof Müller und Ralph Wyss

**Risiko Internet**

gungsbehörden sowie internationale Organisationen zur Verbrechensbekämpfung den Schluss, dass es im Internet noch keine oder erst wenige wirklich grosse Fälle von Wirtschaftskriminalität gebe. Die Masse der Online-Zahlungen sei einfach noch zu gering. Ganz abgesehen davon, dass dieses Argument inzwischen nicht mehr stimmen dürfte: Liegt der Grund nicht vielmehr darin, dass sich Wirtschaftskriminalität von anderen Kriminalitätsformen grundsätzlich unterscheidet und sich daher im Internet völlig anders darstellt?

**Vertrauen und Kontrolle**

Jedes wirtschaftliche Handeln basiert auf einem mehr oder minder grossen Anteil von Vertrauen in den Vertragspartner sowie die dazugehörigen Rahmenbedingungen, namentlich das jeweilige Rechtssystem.

Ein komplettes Ersetzen von Vertrauen durch Kontrolle ist dabei weder möglich noch erwünscht. Auf jeder Stufe der Entwicklung der Zivilgesellschaft mussten daher dieses Vertrauen und die dazugehörigen Kontroll- und Sanktionsmechanismen neu definiert werden.

Die abendländische Zivilrechtslehre ist geradezu geprägt von der Suche nach dieser Balance von Vertrauen und Kontrolle im Wirtschaftsverkehr. Wirtschaftskriminalität ist im Kern nun nicht anders als

der vorsätzliche Missbrauch dieses entgegengebrachten Vertrauens und ist somit jeder wirtschaftlichen Tätigkeit inhärent.

**Internet geschickt zunutze gemacht**

Je grösser und effizienter die Möglichkeiten des legalen Wirtschaftens und das in diese gelegte Vertrauen, desto grösser also sind die Möglichkeiten für Wirtschaftskriminelle, diese auszunutzen. Und hier liegt auch der grosse systematische

Unternehmen schliessen sich zu virtuellen Einkaufsgemeinschaften zusammen oder lassen die Anbieter sich gegenseitig herunterhandeln, um bessere Konditionen zu erhalten; Logistikfirmen verlegen ihre gesamte Kapazitätsplanung auf Internetplattformen und steigern so die Transparenz und Effizienz für die Kundschaft; kleine flexible Firmen schliessen sich zu so genannten virtuellen Gesellschaften zusammen, um je nach Auftrag

in neuer Zusammensetzung das passende Angebot abzugeben; und grosse Produktionsfirmen eröffnen digitale Plattformen sowohl beim Einkauf wie auch beim Vertrieb, um Lager abzubauen und zeit- und nachfragegerecht zu produzieren.

**Justiz ist hilflos**

Es wäre blauäugig zu glauben, dass die Wirtschaftskriminalität sich diesen Möglichkeiten verschliesst. Ganz im Gegenteil: Die mit dem Internet verbundene Automatisierung und Anonymisierung der Wirtschaftsabläufe bietet hervorragende Bedingungen für kriminelle Machenschaften. Und indem der Finanzsektor sogar an vorderster Stelle dieser Entwicklungen steht, ist dafür gesorgt, dass auch die Geldwäsche mit der nötigen Effizienz ablaufen kann.

Während nun aber die legale wie auch die illegale Wirtschaft sich grundlegend verändern, um mit den rasanten Verände-

*Das möglicherweise von philippinischen Informatikstudierenden lancierte Virus «I love you» hat Milliarden-schäden angerichtet. Dies überschattet die Tatsache, dass zunehmend auch gut organisierte Wirtschaftskriminelle ihr Unwesen im Internet treiben. Für ihre Betrugereien malancien sie sich geschickt die immer mehr ins Internet verlagerten Wirtschaftsabläufe zunutze. Der Justiz fehlen bisher griffige Mittel, um dagegen vorzugehen.*

Unterschied zwischen Hackern, Datendiensten und ähnlichen Kleinkriminellen auf der einen und professionell organisierten Wirtschaftskriminellen auf der anderen Seite: Die Kleinen zerstören Daten oder Infrastruktur des Internet, um zum deliktischen Erfolg zu kommen, die Grossen nutzen die technischen Möglichkeiten hingegen geschickt für sich aus. Die Möglichkeiten sind denn auch enorm: Grosse

rungen Schritt zu halten, tut sich in der Strafverfolgung praktisch nichts. Kriminelle Transaktionen, die in Sekundenschnelle über mehrere Server und Landesgrenzen laufen und deren Widerrechtlichkeit erst im gesamten Zusammenhang erkennbar werden, müssen in aufwändigen internationalen Papierverfahren rekonstruiert werden.

Es wundert nicht, dass darunter die Motivation der zuständigen Untersuchungsrichter, überhaupt ein Verfahren einzuleiten, manchmal etwas leidet. Selbst «Kommissar Zufall» hilft da selten weiter, denn wenn die aufgetauchte Spur nicht weiterverfolgt werden kann, fehlt auch die Grundlage zur gross angelegten Strafverfolgung.

Es ist also keineswegs so, dass das Fehlen von Beispielen für gross angelegte Wirtschaftskriminalität im Internet den Schluss zuliesse, dass es sie nicht gibt. Vielmehr ist es den Strafverfolgungsbehörden schlicht und einfach nicht möglich, diese Fälle aufzudecken.

**Für sichere virtuelle Finanzplätze**

Was ist zu tun? Wenn wir nicht eine immer grösser werdende Schattenwirtschaft im Internet dulden wollen, muss der Staat an Spezialisten aufrüsten, sich international so weit als möglich vernetzen und wenn möglich gemeinsam mit anderen Staaten eine dem Stand der Technik entsprechende Logistik aufbauen.

Dabei ist jedoch nicht der permanente Lauschangriff auf das Internet gefragt, sondern das rasche und effiziente Eingreifen des Staates bei Auftreten von Verdachtsmomenten – allerdings unter Wahrung der Bürgerrechte und unter Aufsicht gerichtlicher Organe. Dass dies nicht umsonst zu haben ist, scheint klar. Doch der wirtschaftliche Nutzen wird auch nicht ausbleiben.

Eine effiziente Strafverfolgung von Internet-Sachverhalten sichert der Schweiz wie auch anderen Staaten mit exponierten Finanzplätzen wie zum Beispiel dem Fürstentum Liechtenstein, nicht nur einen sauberen Finanzverkehr im Internet. Sie eröffnet der einheimischen Wirtschaft auch die interessante Möglichkeit, sich als sicherer Hafen für saubere Geschäfte in der virtuellen Welt anzubieten.

Christof Müller, Dr. iur. HSG et Dr. oec. HSG, Certified Fraud Examiner, ist Inhaber von CMC Christof Müller Consulting in St. Gallen und berät Firmen in Prävention und Krisenmanagement im Zusammenhang mit Wirtschaftskriminalität. Zugleich ist er Rechtskonsulent von BBLP Meyer Lustenberger Rechtsanwälte in St. Gallen.

Ralph Wyss, Dr. iur., Fürsprecher, ist Rechtsanwalt bei BBLP Meyer Lustenberger Rechtsanwälte in St. Gallen und beschäftigt sich mit rechtlichen Fragen des Internet.