Misha Glenny

# CyberCrime

## Kriminalität und Krieg im digitalen Zeitalter

DVA
eBooks

selbst wenn das Dokument nur den wöchentlichen Einkaufszettel enthält. Nachdem Regierungen und Unternehmen immer mehr persönliche Informationen über ihre Bürger oder Kunden sammeln, ist Verschlüsselung einer der wenigen Abwehrmechanismen, die dem Einzelnen noch bleiben, um seine Privatsphäre zu schützen. Sie ist aber auch ein unschätzbar wertvolles Instrument für diejenigen, die sich im Web an verbrecherischen Handlungen beteiligen.

Genau wie traditionelle Kriminelle, die Wege entwickeln müssen, um miteinander zu sprechen und so Freunde, Feinde, Polizisten oder Konkurrenten zu erkennen, so stehen auch Cyber-Bösewichter ständig vor der Herausforderung, die Vertrauenswürdigkeit eines Online-Gesprächspartners zu erkennen. Dieses Buch berichtet unter anderem darüber, wie sie Methoden zur gegenseitigen

Identifizierung entwickelten und wie die Polizeikräfte auf der ganzen Welt sich darum bemühten, die Fähigkeit der Hacker zur Erkennung von Ordnungskräften und V-Leuten im Web zu untergraben.

In den 1990er Jahren konnte man das Belauschen krimineller Aktivitäten durch unerwünschte Gäste am einfachsten dadurch verhindern, dass man für Websites, die im Internet der Diskussion von Gesetzesverstößen dienten, ein strenges Überprüfungs- und Mitgliedersystem einführte. Aber trotz solcher Sicherheitsmaßnahmen war es nur eine Frage von Monaten, bis Ordnungsbehörden wie der Secret Service der Vereinigten Staaten oder der KGB-Nachfolger FSB Zugriff auf derartige Seiten hatten; den Zugang hatten sie sich verschafft, indem sie sich geduldig als Verbrecher ausgaben oder indem sie Informanten veranlasst hatten, für sie zu

arbeiten.

Manche Agenten erbrachten dabei so überzeugende Leistungen, dass einige Geheimdienste sogar Mittel bereitstellten, um verdeckte Ermittler ihrer Schwesterorganisationen zu fassen, weil sie annahmen, sie seien echte Kriminelle.

Durch solche Bemühungen haben Polizeikräfte und Spione im Laufe der letzten zehn Jahre eine große Datenbank mit kriminellen Hackern aufgebaut. Darin erfasst sind Nicknames, der tatsächliche oder mutmaßliche Wohnort, kriminelle Aktivitäten und die häufigsten Kommunikationspartner. Dabei wurden die Daten über die unterste Ebene der Cyberkriminellen gründlich durchgekaut. Aber trotz all dieser Informationen ist es nach wie vor äußerst schwierig, Internet-Verbrecher zur Rechenschaft zu ziehen.

Deshalb bereitet das Wesen des Internets – insbesondere seine weltweite Vernetzung – allen Ordnungskräften ungeheures Kopfzerbrechen: Niemand ist jemals zu 100 Prozent sicher, mit wem er oder sie im Web kommuniziert. Haben wir es mit einem Wald-und-Wiesen-Hacker zu tun? Oder mit jemandem, der einflussreiche Freunde an höherer Stelle hat? Sprechen wir mit einem Verbrecher? Oder mit einem Spion? Oder mit einem militärischen Ermittler, der den Wert krimineller Hackermethoden beurteilen will? Beobachten wir den Gesprächspartner oder beobachtet er uns? Will er selbst Geld verdienen? Oder sammelt er Geld für Al-Qaida?

»Das Ganze ist wie ein Schachspiel in sieben Dimensionen«, sagte der Zukunftsforscher Bruno Giussani einmal. »Man ist nie sicher, wo der Gegner sich im Augenblick gerade

befindet.«

Als ich in der Google-Zentrale im kalifornischen Mountain View eintreffe, habe ich nicht ganz das gleiche Gefühl wie damals, als ich zum ersten Mal den Blick auf das Tadsch Mahal richtete, aber ich empfinde doch ein wenig Ehrfurcht. Ich parke auf der Charleston Avenue vor dem bunten Firmenschild, das eines der ehrgeizigsten und erfolgreichsten Projekte der postindustriellen Welt ankündigt.

Die Geschwindigkeit, mit der Google sich in unseren Alltag eingenistet hat – mit allen Höhen und Tiefen, die sich mit der kontrollierten Einnahme eines Rauschmittels verbinden –, sucht ihresgleichen. Die einzigen Konkurrenten sind Angehörige aus der Familie der digitalen Großunternehmen wie Facebook, Microsoft und Amazon. Aber nicht einmal diese drei können einen so großen Erfolg