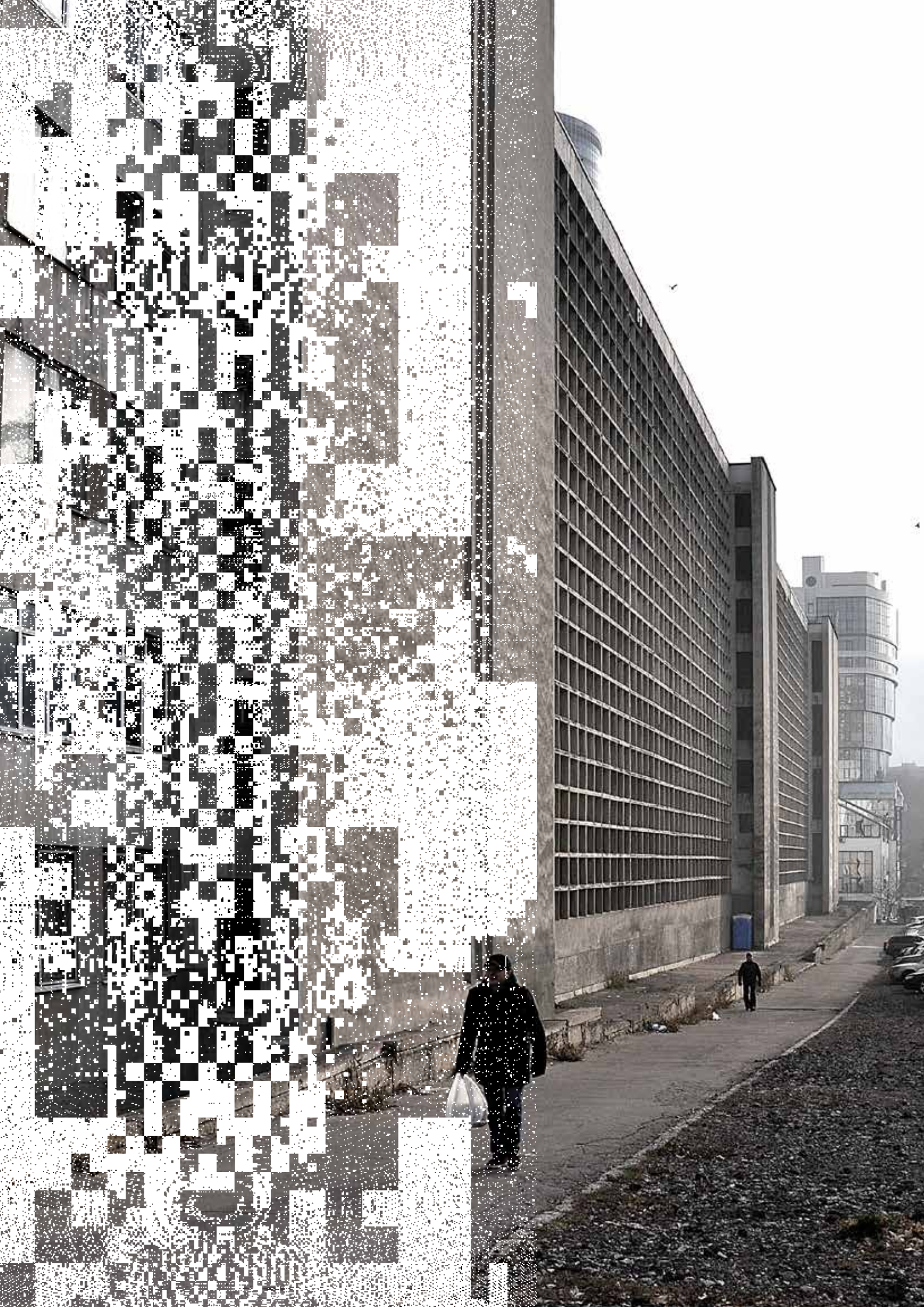
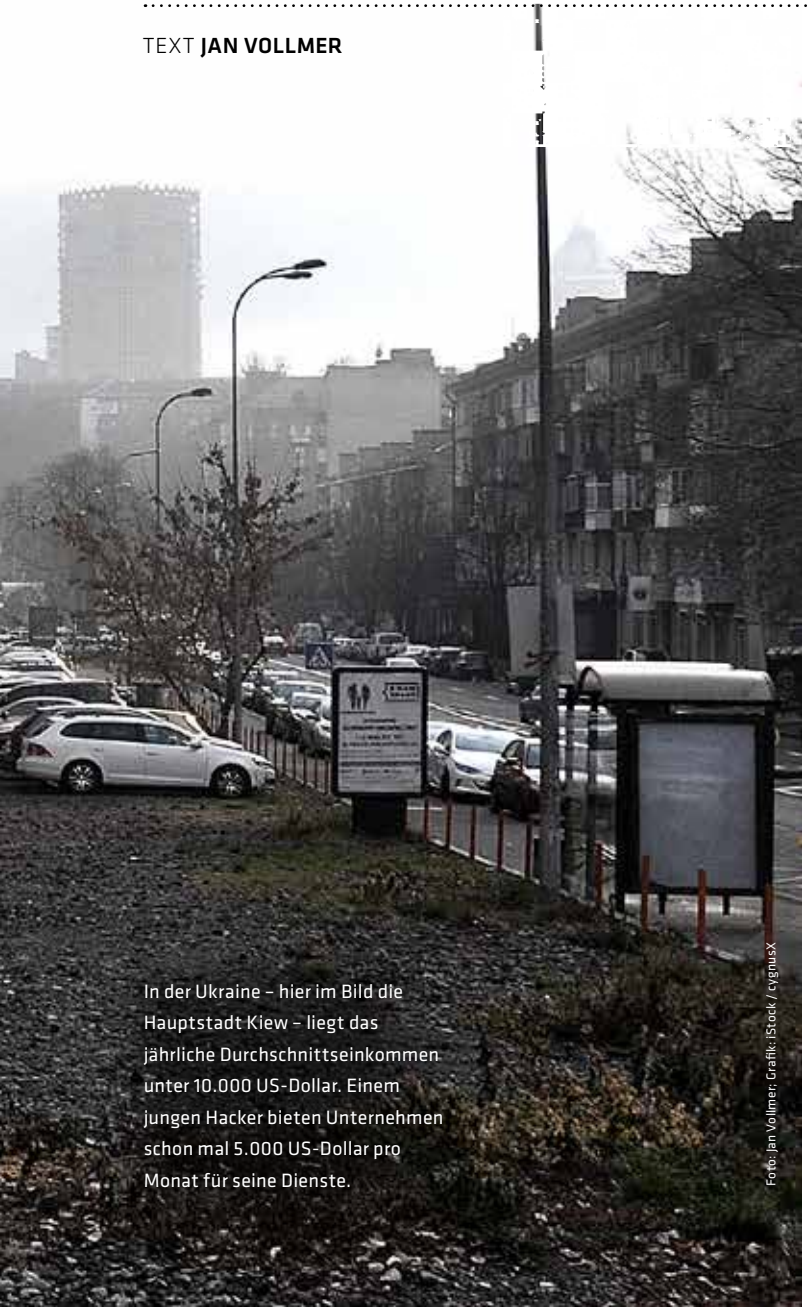


UKRAINE

HACKER'S PARADISE

Die Ukraine war mal ein Hotspot für Kleinkriminelle im Netz. Dann kam der Krieg mit Russland. Heute ist das Land ein Testgelände für den Cyberwar. Und die IT-Sicherheitsindustrie blüht.

TEXT **JAN VOLLMER**



In der Ukraine – hier im Bild die Hauptstadt Kiew – liegt das jährliche Durchschnittseinkommen unter 10.000 US-Dollar. Einem jungen Hacker bieten Unternehmen schon mal 5.000 US-Dollar pro Monat für seine Dienste.

Foto: Jan Vollmer; Grafik: iStock / cygnusX

Artem Afian, ein Mann in seinen 30ern, mit gepflegtem Bart, brauner Weste über dem Hemd und in olivgrünen Hosen, sitzt an einem hölzernen Konferenztisch in seiner Kanzlei in Kiew, im sechsten Stock eines Bürogebäudes. Durch große Fenster kann man runter auf die Straße schauen, über die schwere Geländewagen mit getönten Scheiben donnern: Neue Toyota Landcruiser, Landrover und G-Klassen auf den löchrigen Straßen eines Landes, in dem das jährliche Durchschnittseinkommen unter 10.000 US-Dollar liegt. Hinter Artem an der Wand hängt eine Pop-Art-version des Renaissance-Gemäldes „Das Urteil des Kambyses". Das Bild zeigt, wie der korrupte Richter Sisamnes festgenommen und gehäutet wird, bevor mit seiner Haut der Richterstuhl bespannt wird. „Wir haben eine Kopie auch an die Justiz geschickt, aber da wollten sie es nicht haben", erzählt er und grinst.

Afian hat sich Anfang der 2010er-Jahre auf IT-Recht spezialisiert. Wie sich die ukrainische Cyber-Szene verändert, spiegelt sich in seinen Fällen wider. Zu Beginn riefen private Hacker bei Artem an, wenn überraschend dann doch mal die Polizei vor der Tür stand: Carder aus Odessa, die dabei erwischt wurden, wie sie mit anderer Leute Kreditkartendaten herumhantierten; Data-Miner, die zu tief in fremde Datensätze geschaut hatten. Er vertrat Betreiber von Filesharing-Seiten wie Ex. und andere. Er wurde das erste Mal in Bitcoin bezahlt. Mittlerweile baut Artems Kanzlei auch den legalen Rahmen für Bug-Bounty-Aufträge: Sicherheitstests, die Hacker im Auftrag von Kunden durchführen.

Die klassischen Hacker-Fälle werden in seiner Kanzlei weniger. „Vor fünf oder zehn Jahren war die Ukraine mal so etwas wie ein Hacker-Himmel. Aber die Ära des privaten Hackers geht

zu Ende. Die Carder sind fast verschwunden. Hacking wird jetzt organisierter. Wenn ein Jugendlicher beim Hacken erwischt wird, kommt die Polizei. Und am nächsten Tag schon ein Unternehmen, das ihm 5.000 Dollar im Monat bietet, wenn er dort anfängt."

Diese Evolution hat auch politische Gründe: 2014 hat sich die Ukraine mit der Maidan-Revolution von Russland losgesagt; die Hauptstadt will seitdem auch nicht mehr „Kiew" genannt werden, sondern „Kyjiw", in ukrainischer Schreibweise. Mit der Emanzipation ist das Land zu einem Testgelände für Cyberwaffen geworden. War die Ukraine in den 2000er-Jahren und frühen 2010ern noch ein Spielplatz für private Hacker, tobt dort jetzt ein digitaler Krieg. Mittlerweile schickt auch die USA Cybertruppen in die Ukraine, damit sie dort lernen, wie digitale Angriffe funktionieren, und um sich selbst darauf vorzubereiten. Spätestens seit dem Angriff auf die Server der Demokratischen Partei, der US-Präsident Donald Trump zum Sieg verholfen haben soll, ist auch den USA klar, welche Wirkung Cyberwaffen entfalten können.

Es ist zwar fast unmöglich, Cyberangriffe klar einem Staat und einer Kommandostruktur zuzuordnen. Die Möglichkeit, sie abstreiten zu können, ist schließlich von Anfang an in den Attacken eingepreist. Bei den großen Angriffen in der Ukraine erkennen Experten und Geheimdienstmitarbeiter aber klar eine russische Handschrift.

EIN WURM, DER MILLIARDEN KOSTETE

Der bisherige Höhepunkt auf dem Testgelände Ukraine war „Notpetya": Ein Wurm, der im Sommer 2017 von einem gehackten Server einer kleinen Kiewer Software-Schmiede ein ganzes Land lahmlegte. Der Wurm vernichtete nach Schätzungen die Daten von zehn Prozent aller Computer der Ukraine und legte dort zwischenzeitlich zwei Flughäfen, 22 Banken und etliche Behörden lahm. Von ukrainischen Rechnern sprang Notpetya über auf die Firmenrechner von Konzernen wie dem Pharmariesen Merck oder den Logistikern Fedex und Maersk. Den US-Konzern Merck soll Notpetya laut Schätzungen des US-Experten Andy Greenberg 870 Millionen US-Dollar gekostet haben. Bei Maersk, der weltweit größten Container-Reederei, soll der Wurm ein 300 Millionen-Dollar-Loch gerissen haben. Sicherheitsexperten aus dem Weißen Haus bezifferten den Gesamtschaden später auf etwa zehn Milliarden US-Dollar – und beschuldigten den russischen Geheimdienst GRU. Notpetya gilt bis dato als der verheerendste Hack der Welt.

Die konstante Gefahr für ukrainische IT–Systeme hat IT-Sicherheit aber auch zu einem zentralen Thema gemacht: Aus der klassischen Software-Outsourcing-Industrie ist ein florierender Cybersecurity-Sektor erwachsen. Hacker und IT-Security-Experten arbeiten jetzt für die Regierung und ziehen zunehmend auch internationale Aufträge an Land.

In einem Café namens „The Cake" in der Kiewer Innenstadt sitzt Victor Zhora und isst Kuchen. Er ist Ende dreißig und trägt einen schwarzen Rollkragenpullover. Neben unserem Tisch steht eine in Pink glänzende, zwei Meter große Hundeskulptur aus Plastik, die an die Arbeiten des US-Künstlers Jeff Koons erinnert und dem Gespräch einen etwas surrealen Touch verleiht.

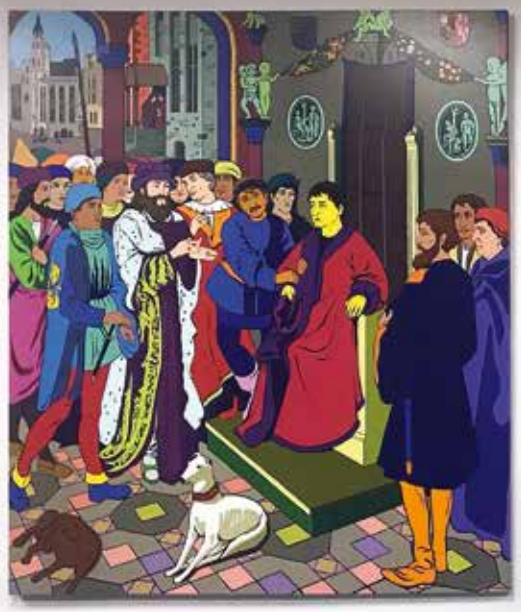
Zhora arbeitet seit den 2000ern in der ukrainischen IT-Sicherheit. „Vor 15 Jahren war so was wie ‚Cyberwar' noch kein Thema", erzählt er und gabelt sich ein Stück von dem Karottenkuchen vor ihm auf dem Tisch. Seitdem sich die Ukraine politisch von Russland entfernt, hat sich das geändert. Mittlerweile hat er mitgeholfen, acht Parlaments- und Präsidentschaftswahlen digital zu sichern –, seit 2009 mit seiner eigenen Firma Infosafe. Eigentlich wird in der Ukraine noch auf Papier gewählt, das Endergebnis der Wahlen ist damit schwer digital zu hacken. Aber in einem Land, das seit 2004 zwei Revolutionen erlebt hat, können schon Unklarheiten in der Wahlnacht zu erhitzten Gemütern führen. „Auf der Website der Wahlkommission gab es in der Wahlnacht und am nächsten Tag wahnsinnig viel Traffic", sagt Zhora. „Die Website wurde permanent angegriffen. Wir versuchten sie dann mit allen Mitteln – von Web-Mirroring bis DDoS-Abwehr – aufrechtzuerhalten."

Die intensivsten Angriffe hat Zhora am 25. Mai 2014 erlebt. „Unser großer Nachbar hatte sich damals entschieden, dem Rest der Welt zu beweisen, dass wir eine Junta in Kiew gewählt hätten", erzählt er. Junta ist der Begriff, den 2014 vor allem russische Medien nutzten, um die damalige ukrainische Verwaltung zu diskreditieren. „Bei dem Angriff gab es drei Phasen", erzählt Zhora. Schon vor der Wahl waren Hacker mit gezielten Phishing-Angriffen unbemerkt in das Computersystem der Wahlkommission eingedrungen. Nur Stunden bevor die ersten Hochrechnungen auf der Website der Wahlkommission veröffentlicht wurden, bekamen er und seine Kollegen einen Tipp. Jemand hatte festgestellt, dass schon vor den ersten Hochrechnungen ein Bild von einem vermeintlichen Wahlsieger auf der Seite hochgeladen worden war, und damit jederzeit veröffentlicht werden konnte. Darauf zu sehen: Dmytro Jarosch, Anführer der rechtsradikalen Paramilitärs „Prawyj Sektor" (dt.: rechter Sektor).

Ein Bild von Jarosch als Wahlgewinner auf der offiziellen Seite der Wahlkommission hätte katastrophale Folgen für die Ukraine gehabt: Russische Medien, die auch in der Ukraine viele Zuschauer haben, hätten damit ihrer Junta-These neuen Aufwind verliehen. Die Nachricht von Jarosch als Gewinner hätte in kürzester Zeit sowohl die Paramilitärs des „Prawyj Sektor" und die fassungslosen Anhänger der anderen Parteien auf die Straße gebracht: Ein Chaos, das die ganze Wahl infrage gestellt hätte.

„Unser großer Nachbar hatte sich damals entschieden, dem Rest der Welt zu beweisen, dass wir eine Junta in Kiew gewählt hätten."

„Als wir das Bild sahen, war uns klar, dass das System kompromittiert worden war", erzählt Zhora. Das System komplett zu checken und den Angreifer mit Sicherheit rauszuschmeißen, hätte zu lange gedauert. „Also begannen wir, alle Knotenpunkte und die Website komplett auszutauschen", erzählt er. Die neue Website ging erst kurz vor den ersten Hochrechnungen online. „Der einzige Aufruf des alten Links zu der Seite, wo Jaroschs Bild gewesen



Oben: Der Anwalt der Hacker: Der Ukrainer Artem Afian hat sich auf IT-Recht spezialisiert. Waren früher Data-Miner und File-Sharer unter seinen Mandanten, sind es heute Unternehmen, die Hacker für Sicherheitstests engagieren wollen.

Links: Im Mai 2014 zählen freiwillige Helfer die Wahlzettel in der Präsidentschaftswahl aus. In der Wahlnacht wurde die Webseite der Wahlkommission permanent angegriffen. Es waren bisher die intensivsten Hacker-Angriffe in der ukrainischen Geschichte.

Fotos: Jan Vollmer, Shutterstock / snig

Yegor Aushev und Evgenia Brosheva (v.l.) sind die Chefs der Plattform Hacken Proof, die die Dienste von rund 3.000 Hackern an Unternehmen vermittelt. Vasyl Zadvorny (r.) ist CEO der E-Procurement-Plattform Prozorro.

wäre, kam von der IP-Adresse eines russischen Fernsehsenders", sagt Zhora mit vielsagendem Blick. Der Hack der Website der ukrainischen Wahlkommission war so etwas wie der Startschuss der großen politischen Cyberangriffe auf die Ukraine.

Am 23. Dezember 2015 ging für 230.000 Anwohner in der westlichen ukrainischen Region Iwano-Frankiwsk am frühen Abend plötzlich das Licht aus. In einer hochkomplexen Operation hatten zum ersten Mal weltweit Hacker die Kontrolle über ein Stromnetz übernommen. Und sie waren gut vorbereitet. Mit einem per E-Mail verschickten Word-Exploit namens „Blackenergy3" hatten sie schon im Frühling 2015 angefangen, die Rechner von Mitarbeitern von Stromversorgern in der westlichen Ukraine zu infizieren.

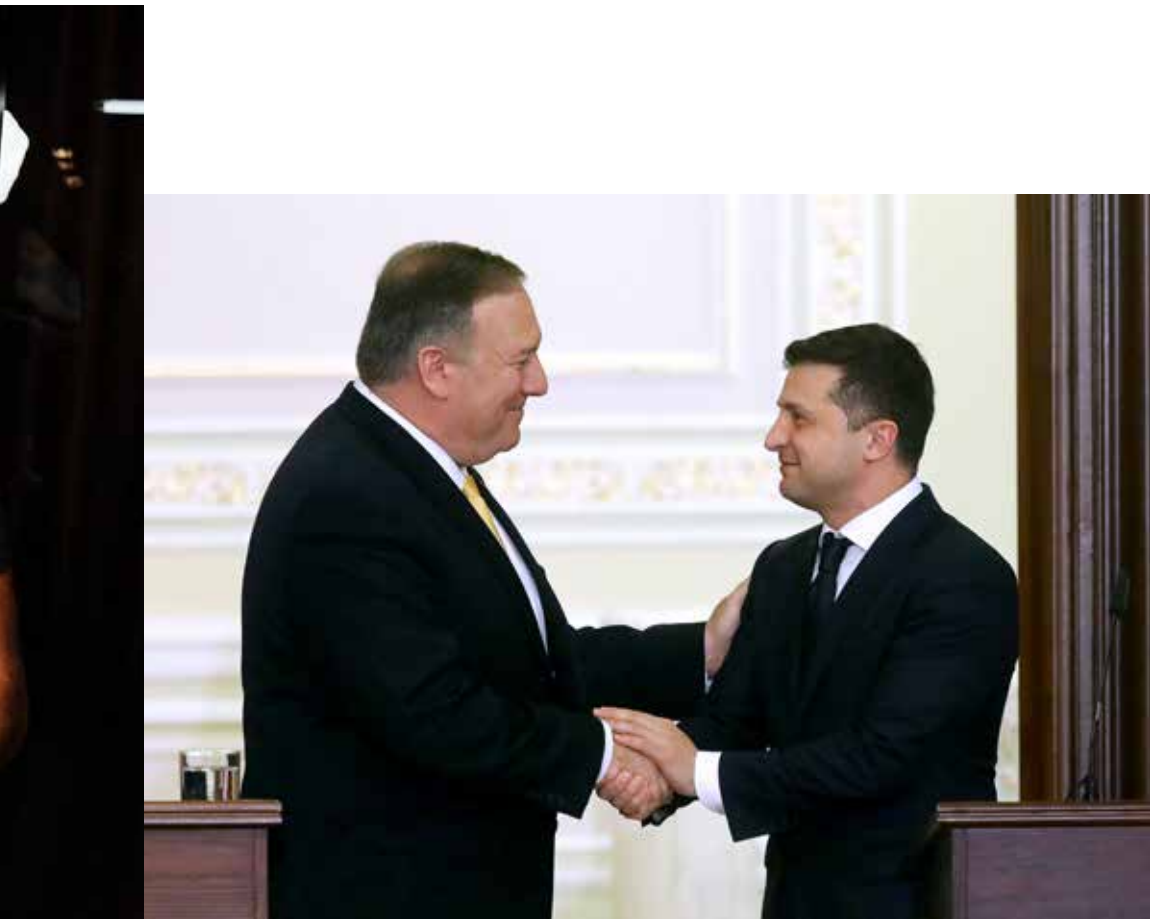
Die Hacker haben Monate damit verbracht, Firewalls der Stromversorger zu umgehen, und sich mit den Industriecomputern und ihren Funktionen vertraut zu machen. Bis es am 23. Dezember 2015 so weit war – und sie bei drei Verteilerzentren und 30 Unterzentren den Hebel umlegten – und den Strom abstellten. Als Kür legten die Hacker während des Angriffs noch die Notstromaggregate der drei angegriffen Verteilerzentren lahm, sodass selbst die ohnehin schon verwirrten Mitarbeiter der Stadtwerke im Dunkeln saßen.

Auf den Blackenergy-Hack folgte etwa ein Jahr später, im Dezember 2016, der Hack auf den Kiewer Stromanbieter „Kyivenergo". „Dabei ging im Norden von Kiew das Licht aus. Die Malware, die dabei benutzt wurde, wurde speziell für die industriellen Kontrollsysteme von Kyivenergo geschrieben", erzählt Zhora. „Wenn du etwas hast, das in so einem System funktioniert, kannst du es hier ausprobieren und woanders wirklich einsetzen."

Aber nicht nur die Angreifer üben in der Ukraine. Seit den Hacks auf die Wahlen und Energiesysteme schicken die USA nicht nur Equipment und Unterstützung zur Abwehr –, sondern auch Cyberspezialeinheiten, die die Angriffe selbst vor Ort studieren, um die USA darauf vorzubereiten. „Unsere Lösung für den Blackenergy-Hack war, den Storm in den Verteilerzentren wieder manuell anzustellen. In den USA würde das gar nicht mehr gehen, dort wird das Stromnetz komplett digital gesteuert", sagt Zhora.

„Die USA können in der Ukraine beobachten, wie Systeme angegriffen werden, und so die Taktik der Angreifer studieren."

„Es ist wahrscheinlich, dass die Hacker sehen wollten, ob die Malware so funktioniert, wie sie soll. Und auch, wie die internationale Gemeinschaft darauf reagieren würde", erklärt mir Marie Baezner in einem Skype-Anruf. Baezner forscht am Center for Security Studies der ETH Zürich zur Frage, welche Rolle



Verbündete im Cyberkrieg: Der US-amerikanische Außenminister Mike Pompeo (links) trifft den ukrainischen Präsidenten Wolodymyr Selenskyj in der Hauptstadt Kiew.

Cyberangriffe in Konflikten wie den Kriegen in Syrien oder der Ukraine spielen. Sie zählt in einem ihrer wissenschaftlichen Artikel 64 Angriffe und Gegenschläge im Ukraine-Konflikt zwischen November 2013 und Dezember 2016. „Die Ukraine hat definitiv einen strategischen Wert für die USA. Die USA können in der Ukraine beobachten, wie die Systeme angegriffen wurden, welche Malware verwendet wurde, und die Taktik der Angreifer studieren. Es war hilfreich, das vor den Midterm-Wahlen 2018 zu sehen. Sie werden das Gleiche vor den Wahlen 2020 tun und Cybertruppen in die Ukraine, Mazedonien und Montenegro schicken."

In einer vernetzten Welt bleiben Cyberangriffe auf Staaten nicht dort, wo sie anfangen. Nur ein paar Kilometer von dem Café „Cake" entfernt, in dem ich Victor Zhora treffe, arbeitet die kleine ukrainische Software-Schmiede namens „Linkos Group". Linkos verkauft ein unscheinbares Buchhaltungsprogramm namens M.E.Doc, vor allem an ukrainische Kunden. Im Juni 2017 nutzen Hacker einen der Linkos-Server, um den Wurm, der später als „Notpetya" bekannt wurde, auf die Welt loszulassen.

Die Hacker-Angriffe auf die Ukraine, die Security-Experte Zhora „eine kalte Dusche" nennt, hatten auf die ukrainische Hacker-Szene aber auch einen vitalisierenden Effekt. Im Westen Kiews, in einem Café in einem IT-Hub namens „Unit City" treffe ich Yegor Aushev und seine Geschäftspartnerin Evgenia Brosheva. Beide tragen Kapuzenpullover, Aushev in Schwarz, Brosheva in Rot. Mit Geld aus einem frühen Krypto-ICO haben die beiden eine Plattform namens „Hacken Proof" aufgebaut. Auf der Plattform können Unternehmen sich für einen Penetration-Test anmelden: gewissermaßen ein „Hackbarkeitstest". Einer der rund 3.000 auf der Seite angemeldeten legalen Hacker sucht dann nach Schwachstellen im jeweiligen Unternehmen – und protokolliert, was er findet.

Die wechselhafte Geschichte der Ukraine vom ehemaligen Hotspot für Cyberkleinkriminelle zum gebrannten Kind des Cyberkrieges hat sein Geschäft in Schwung gebracht. „Es hat lange gedauert, um Leute zu überzeugen, das erste Mal eine ukrainische Cybersecurity-Firma anzuheuern. Andererseits ist die Ukraine mittlerweile für ihre Hacks und Hacker bekannt", erklärt Aushev. Ein Kunde, auf den er besonders stolz ist, ist eine asiatische Airline. Es gibt keine offiziellen Zahlen, aber Hacken-Proof-Gründer Aushev schätzt, dass es in der Ukraine rund 30 Cybersecurity-Unternehmen gibt. Dabei hat er die steigende Nachfrage nach Sicherheitsspezialisten als eigenes Geschäftsfeld entdeckt – und IT-Security-Kurse ins Portfolio seines Unternehmens aufgenommen. Nicht zuletzt wegen Hacks wie Blackeenergy und Notpetya boomt die Sicherheitsindustrie wie nie zuvor. Und ukrainische Hacker sind im Feuer des Cyberkriegs zu ihrer eigenen Marke geworden.

JAN VOLLMER ist als Digital-Reporter für t3n auch viel international unterwegs. Bei seiner Recherche in der Ukraine hat ihn überrascht, dass ukrainische Hacker wirklich gern Kapuzenpullover tragen.

Fotos: Yegor Aushev, Picture Alliance / Pyotr Sivkov / TASS / dpa