
DIE CYBER-KRIEGERINNEN

TEXT: EVA STEINLEIN ILLUSTRATIONEN: PAUL PAETZEL

CYBER-ATTACKEN sind längst keine Science-Fiction mehr – nicht nur bei US-Wahlen. Auch Estland, Lettland und Litauen sind das Ziel von digitalen Angriffen. Gegen russische Hacker und Propagandakampagnen kämpfen junge Frauen im Baltikum ganz vorn an der unsichtbaren Front

Sille Laks verteidigt Estland, seit sie 17 Jahre alt ist. Da hat ihr Großvater sie zum ersten Mal auf ein Wochenende mit dem Verteidigungsbund mitgenommen, einem Paramilitär, das an die estnischen Streitkräfte angeschlossen ist. Mit anderen Freiwilligen geht sie seitdem regelmäßig auf kilometerlange Märsche und Bergtouren, hebt Gräben aus, übt Schießen mit dem Luftgewehr, übernachtet im Wald. „Noch am ersten Sonntagabend habe ich meine Beitrittserklärung auf der Webseite ausgefüllt", erinnert sich die 32-Jährige, die ihre verspiegelte Sonnenbrille am liebsten nie absetzt. Nun ist sie eine von fast 26 000 Esten, die samt der Frauen- und Jugendorganisationen zum Verteidigungsbund gehören und im Kriegsfall als Reservisten kämpfen sollen. Eine beachtliche Verstärkung des Militärs in dem kleinen baltischen Staat, der nur 1,3 Millionen Einwohner und 6000 aktive Soldaten zählt. Bis 2020 wollen die baltischen Streitkräfte auch ein Cyberkommando von 300 Personen aufgebaut haben. Der paramilitärische estnische Verteidigungsbund hat schon seit mehreren Jahren eine Cybereinheit, in der auch Laks sich engagiert.

Den größten Teil seiner Geschichte hat Estland ebenso wie Lettland und Litauen unter wechselnder Herrschaft verbracht, von 1940 bis 1991 gehörte das Land zur Sowjetunion. Die meisten Balten nennen diese Zeit „die Okkupation" und ohne jene Besatzung – so der Vorwurf – hätte die Region heute den Entwicklungs- und Lebensstandard Skandinaviens. Spätestens seit der Annexion der Krim und dem Konflikt in der Ukraine treibt nun immer mehr Balten die Sorge um, sie könnten von ihrem gemeinsamen Nachbarn Russland erneut okkupiert werden.

Sille Laks ist nicht einmal 50 Kilometer von der russischen Grenze entfernt aufgewachsen. Ihren ersten Einsatz für die Verteidigungseinheit hatte die energische IT-Expertin 2007 als Hilfspolizistin. In der Nacht auf den 27. April waren in den Straßen der Hauptstadt Tallinn und in ihrer Heimatstadt Jõhvi schwere Unruhen zwischen ethnischen Russen und Esten ausgebrochen.

Nach der Unabhängigkeit des Landes 1991 hatte man die ethnischen Russen und ihre Nachfahren, die in Estland und Lettland immerhin ein Viertel der Bevölkerung ausmachen, zu „Nichtbürgern" erklärt. Bis heute dürfen sie weder wählen noch im öffentlichen Dienst arbeiten, die „Naturalisierung" genannte Einbürgerung ist ein kompliziertes bürokratisches Verfahren. In den Krawallen von 2007 brach sich ihre aufgestaute Wut explosionsartig Bahn.

Doch die eigentliche Bedrohung waren nicht die Kämpfe auf der Straße – sie kam aus einem Angriffsfeld, mit dem bis dahin kaum jemand gerechnet hatte: dem Internet. Russische Hacker legten mit einer Flut automatisierter Aufrufe gezielt die Webseiten wichtiger Staatsorgane, Banken und Nachrichtenmedien lahm. Später kaperten sie die Seiten und luden dort politische Parolen und Propagandabilder hoch. In einem Land, dessen Bürger schon damals online an Wahlen teilnehmen, Behördengänge und Arztkonsultationen erledigen konnten, war das mehr als ein Weckruf: Der Cyberangriff traf das Selbstverständnis Estlands als digitale Nation im Kern.

Die Esten mussten dringend umdenken: Cybersicherheit hat seitdem oberste Priorität. Sille Laks hat den Prozess von Anfang an auf höchster Ebene mitgestaltet. Sie sitzt in der Halle der Technischen Universität Tallinn, an der sie ihren Master in Cybersecurity gemacht hat und heute „Grundlagen der Cybersicherheit" unterrichtet, lehnt sich tief in den gepolsterten Stuhl und erzählt: Vier Jahre lang hat sie in der Notfall-Eingreiftruppe der staatlichen IT-Sicherheit gearbeitet – einer Behörde, die mit dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) vergleichbar ist. Dort werden einheitliche Sicherheitsstandards für die estnische Regierung bei Passwörtern, Software und Reporting festgelegt. Auf Backup-Servern in Luxemburg ist zudem der gesamte Datensatz aller Bürger abrufbar, falls Estlands digitale Infrastruktur zum Erliegen kommt.

Auch der paramilitärische estnische Verteidigungsbund zog seine Schlüsse und richtete eine Cybereinheit ein, der heute etwa 200 Personen angehören. Sille Laks ist aktives Mitglied dieser „Küberkaitseliit" und nimmt an Übungen teil, mit denen die Einheit und die staatliche IT-Sicherheit gemeinsam den Kampf gegen Hackerangriffe trainieren: Eine Gruppe attackiert etwa den Server einer Klinik in der Küstenstadt Pärnu, die andere Gruppe muss den Angriff abwehren – und dabei neben logistischen Fragen auch bedenken, was sie wann an die Öffentlichkeit kommuniziert.

„Wir haben gelernt, dass man tatsächlich ein ganzes Land aus dem Netz angreifen kann – und dass wir etwas dagegen tun müssen", sagt Sille Laks, die ein T-Shirt mit der Aufschrift „Just nerd faster" trägt. Sie strahlt den gleichen Pragmatismus aus, der auch Estland

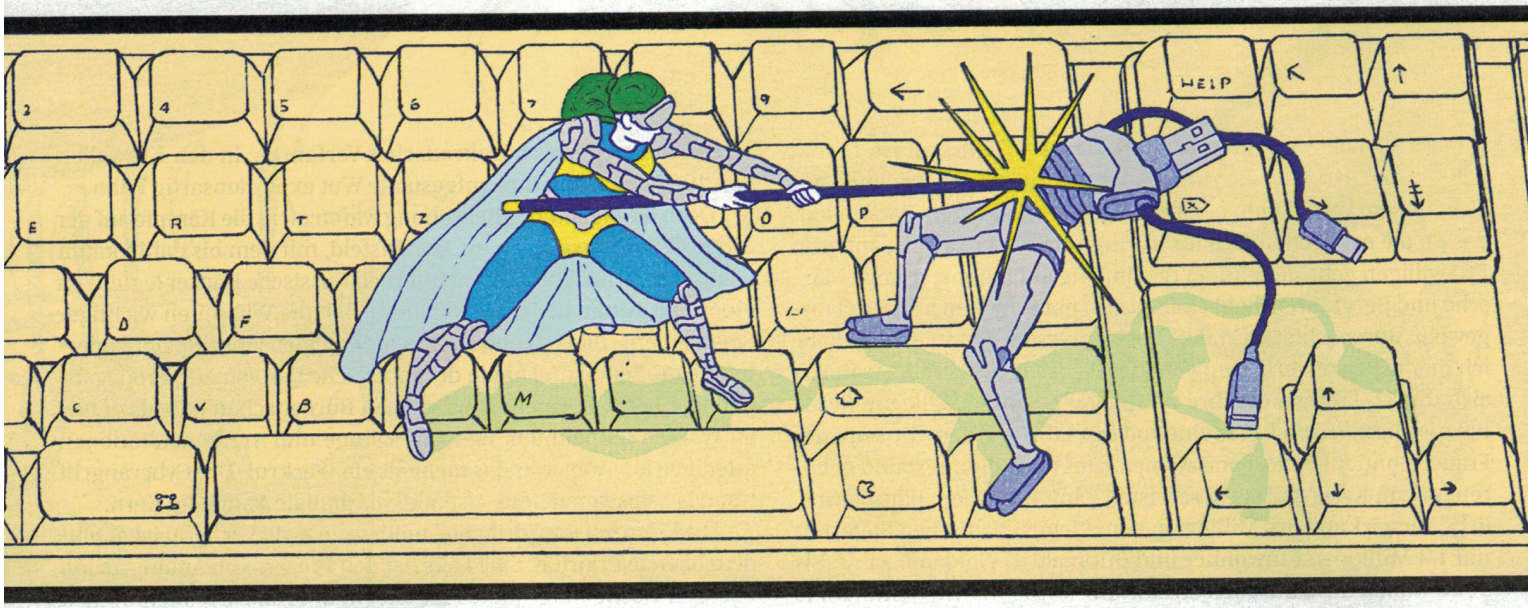
als Cyberbastion ausmacht. Emotional wird sie nur, wenn sie sich über den unbedarften Umgang der Deutschen mit Sicherheitsfragen wundert, den sie bei einem Behördengang bemerkt hat: „Da hatten sie noch Computer mit Windows XP Home Edition, von denen einer zehn Minuten lang entsperrt und unbeobachtet vor mir stand."

Dass ein System verwendet wird, für das es keine Updates mehr gibt, ist jemandem wie Sille Laks wesensfremd. Alles an ihr signalisiert Zielstrebigkeit: ihr Gang, ihre Sprechweise, ihre Laufbahn in der Tech-Branche, die sie selbst nicht als bemerkenswert ansieht.

Denn während man in Deutschland überlegt, wie man Frauen fördert, sind die Balten schon weiter: Obwohl die Beschäftigungsquote unter Frauen niedriger ist als in Deutschland, haben alle drei Länder einen höheren Frauenanteil auf mittleren und höheren Führungspositionen – Lettland ist mit fast 44 Prozent sogar EU-Spitzenreiter. Das liegt zum einen daran, dass deutlich mehr Frauen heute ist. Barojan nennt sich selbst „Digital Sherlock": Sie spürt Desinformationskampagnen im Internet auf und versucht, mit Software-Tools den Methoden der Urheber auf den Grund zu gehen.

Denn längst findet neben dem Cyberkrieg der Hacker auch eine Propagandaschlacht statt, deren Beteiligte alles andere als im Verborgenen agieren: Kremlnahe Medien wie Sputnik und RT beeinflussen nicht nur im Baltikum die Debatte über Ereignisse im Weltgeschehen – und ihre Deutung.

Die in Litauen geborene Donara Barojan, die Internationale Beziehungen an der London School of Economics studiert hat, arbeitete 2016 bei einer Kommunikationsberater-Firma in Großbritannien und bekam verwundert mit, wie ihre Verwandten in der Heimat immer öfter kremlfreundliche Artikel posteten. „Ich habe sie darauf angesprochen und bekam als Antwort: ‚Na ja, das taucht oft in meiner Timeline auf, und ich fand es wichtig, das zu teilen.'"



als Männer in den baltischen Staaten einen Hochschulabschluss haben. Zudem haben die meisten von ihnen neben einem „Just do it"-Pragmatismus auch das Konzept lebenslangen Lernens verinnerlicht: Wieso sollte ein Kind oder eine Umschulung der Grund sein, beruflich kürzerzutreten?

Bei Sicherheitstrainings bringt Sille Laks ihren Zuhörern bei, wie sie sich im digitalen Raum vor Angriffen schützen. Im Anschluss ist sie ansprechbar für Fragen – und bleibt auch mal sechs Stunden länger als geplant: „Ich bin für sie da, nicht sie für mich." Auch im fortschrittlichen Estland gibt es Leute, denen sie erklären muss, wie man Passwörter ändert, eine Spam-Mail erkennt oder wozu eine Zwei-Faktor-Authentifizierung, also ein sicheres Login-Verfahren über zwei Komponenten wie EC-Karte und TAN, gut ist. „Cybersicherheit ist eine gemeinsame Verantwortung", ist sie überzeugt. „Wenn du einen gewöhnlichen Internetnutzer davon abhältst, ein schwaches Passwort zu benutzen, musst du einen Problemfall weniger betreuen."

Die Arbeit von Donara Barojan im Nachbarstaat Lettland setzt einen Schritt früher an. Die Analytikerin sitzt im Konferenzraum des NATO-Exzellenzzentrums für strategische Kommunikation in der lettischen Hauptstadt Riga, wo sie eine Abteilung für Forensik im Netz aufgebaut hat, deren Vizechefin sie

Dass es so leicht ist, auf die Berichte hereinzufallen, ist kein Zufall. „Russland nutzt die Schwachstellen unserer Medienlandschaft sehr geschickt aus", sagt Donara Barojan und klickt als Beleg durch eine Fülle von Tabellen und Analysen, die sie verfasst hat. Sie weiß, wie sie glaubwürdig auftritt: Im Gespräch gestikuliert sie kaum, ihre Miene bleibt stets freundlich-unaufgeregt, selbst ihr auffälliges blaues Brillengestell lenkt nicht von der Sache ab, um die es geht.

Ausführlich schildert sie die Lücken, die sie bei ihrer Arbeit aufgedeckt hat: Sputnik und RT sind Meister darin, durch präzise und informative Berichterstattung in einigen Bereichen Glaubwürdigkeit aufzubauen – sowohl bei ihren Lesern als auch im Algorithmus der sozialen Netzwerke. Steht Russland dann während einer Krise im Medienfokus, veröffentlichen sie staatlich geförderte Propaganda. „Sie vermischen Wahrheit und Lüge und stehen im Ergebnis als verlässliche Nachrichtenquelle da, obwohl sie das nicht sind", erklärt die 26-jährige Analytikerin in britisch gefärbtem Englisch.

Vor zwei Jahren fasste Donara Barojan den Entschluss, London zu verlassen und ins Baltikum zurückzukehren, um den wachsenden Desinformationsoffensiven etwas entgegenzusetzen. Gemeinsam mit anderen „Digital Sherlocks" hat sie die digitale Forensik von einer Art Start-up am NATO-Exzellenzzentrum in Riga zur festen Abteilung ausgebaut, in der auch viele Frauen arbeiten. Als

Grundlage diente den Analysten häufig Software aus dem Marketing, die sie für ihre Zwecke angepasst und weiterentwickelt haben – etwa ein Frühwarnsystem für Fake-News-Kampagnen, das automatisch einschlägige Seiten durchforstet.

Im Baltikum, wo außer der russischen Minderheit auch viele ethnische Esten, Letten und Litauer seit ihrer Schulzeit Russisch können, gewinnen kremlnahe Medien ihr Publikum oft durch Unterhaltungssendungen, in die auf humorvoller Ebene politische Botschaften einfließen. Jüngere Nutzer erreichen sie über die sozialen Netzwerke: Nicht nur die Plattform Twitter ist anfällig für Bots, die beispielsweise durch automatisierte Massenposts einen bestimmten Hashtag populär werden lassen und so künstlich Aufmerksamkeit für ein Thema erzeugen können.

Im Moment entwickelt Donara Barojans Team einen eigenen Bot: Er soll URLs identifizieren können, die auf Fake-News-Meldungen

In Estland werden Behördengänge, Arztkonsultationen und sogar Wahlen online durchgeführt. Um russische Cyberangriffe abzuwehren, engagieren sich Hunderte Freiwillige in einer paramilitärischen Cybereinheit, der „Küberkaitseliit“

führen. Wird ein solcher Link auf Twitter geteilt, soll der NATO-Bot automatisiert eine Antwort unter den Tweet posten: „Hi! Dieser Link führt zu einer Falschnachricht. Hier ist ein Artikel, der sie widerlegt.“ Barojan glaubt, dass es kein Zufall ist, dass solche Technologien ausgerechnet in ihrem Land entwickelt werden: „Ich denke nicht, dass die baltischen Staaten die anfälligsten für russische Desinformation in Europa sind – eher sind sie die widerstandsfähigsten.“ Lange habe die NATO das Baltikum als schwächstes Glied angesehen, dabei hätten die Menschen dort gerade durch die gefühlte Bedrohung eine starke Urteilsfähigkeit und Resilienz im Umgang mit Cyberkampagnen entwickelt, die sie an die Welt weitergeben könnten. Das gelte vor allem für ihre Heimat Litauen: „Wann immer eine Fake-News-Geschichte die NATO-Soldaten in Litauen oder Litauens internationale Position ins Visier nimmt, ist die entlarvte Version der Geschichte tausendmal so populär.“

EVA STEINLEIN

begann ihre Recherche, als gefühlt das ganze Baltikum im Jahresurlaub war. Bester Zeitpunkt für einen Hackerangriff also: im Hochsommer.