

Steirische Friedensplattform: Rede vor der Stiftskaserne, 3.8.20, Wien

Wir stehen hier vor dem **Informations-Kommunikations-Technologie und Cybersicherheitszentrum, einer Abteilung des Österreichischen Bundesheeres**.

Seine Aufgaben lesen sich im Internet nachvollziehbar, wie

- Betrieb eines zentralen Rechenzentrums oder
- Dienstleistungen im Bereich des militärischen Geowesens

Recherchiert man weiter, finden sich dann doch Aufgaben wie

- Cyber Sicherheitsmanagement
- Cyber Security Operations
- Electronic Warfare Operational Support Center

Beim Wort Electronic Warfare gilt es aufzumerken, denn da geht es nicht mehr um „Security“ und „Defense“, sondern um **Kriegsführung**:

Elektronische Kriegsführung (EW) ist jede Handlung, die die Nutzung des elektromagnetischen Spektrums (EM-Spektrum) oder gerichteter Energie beinhaltet, um das Spektrum zu kontrollieren, einen Feind anzugreifen ...¹

Wir wundern uns: Seit wann darf Österreich „einen Feind angreifen“?

Hat man uns nicht seit der Volksschule erzählt, Österreich sei ein neutrales

Land? Das Bundesheer habe die Aufgabe der „Landes**verteidigung**“. Das

Bundesverfassungsgesetz verbietet den Beitritt zu Militärbündnissen und die Errichtung von fremden Militärstützpunkten auf österreichischem Gebiet.

Geht Österreich mit Israel solche Art von Kooperationen ein, die als Errichtung eines fremden „Militärstützpunktes auf österr. Gebiet“ gewertet werden können?

Es ist weithin unbekannt, dass die deutsche Bundeswehr ein Manöver zur Reaktion auf Cyberangriffe in München durchführt. Die Mitbeteiligten sind Österreich und Israel! KennerInnen gehen davon aus, dass „Hack Backs“ trainiert werden.

Was ist ein **Hack-Back**?

Es wird als „aktive Cyberabwehr“ beschrieben, ist aber nichts anderes als ein Einhacken in fremde IT-Systeme. So soll im Falle eines digitalen Angriffs, z.B. auf Stromnetze oder andere wichtige Teile der Infrastruktur, nicht nur verteidigt, sondern angegriffen werden, also zurückgehackt. Wenn nun fremde IT-Systeme durch so ein „Hack-Back“ zerstört werden, kann das weitreichende Folgen haben. Solch ein fremdes IT-System kann nämlich ein für den Angriff gekapertes Krankenhaus sein und dann wären die Auswirkungen verheerend. Ein Hack-Back kann das System völlig zerstören.

Oder was, wenn das fremde System zurückhackt? Eine hochgefährliche Eskalationsspirale mit unübersehbaren Folgen wäre in Gang gesetzt.

¹ https://en.wikipedia.org/wiki/Electronic_warfare und

Electronic Warfare oder „Elektronische Kampfführung ist die Gesamtheit aller militärischen Maßnahmen unter Ausnützung elektromagnetischer Strahlung –zur Informationsgewinnung über den Gegner –zur Verhinderung der Nutzung des elektromagnetischen Spektrum durch den Gegner sowie zur Sicherstellung der Nutzung des elektromagnetischen Spektrums für eigene Anwendungen. Zit. in

https://www.bundesheer.at/pdf_pool/publikationen/diplomarbeit_informationskrieg_publication_lvak_20100902.pdf, S. 62

Deshalb warnen ExpertInnen eindringlich vor dem Einsatz einer solchen Software!

Ein weiterer Grund ist, dass es für den Einsatz dieser Hack Backs bestimmte Programme zu kaufen gibt. Hier kommt **die israelische Firma NSO** ins Spiel. Sie ist Spezialistin für Kauf und Verkauf von Codes, die das Eindringen in Sicherheitslücken von Systemen ermöglichen. Wer diese Codes besitzt, hat eine extrem erpresserische Waffe in der Hand und es nicht gesagt, dass diese Codes nur einmal verkauft werden.

Das Bundesheer würde auch **das Völkerrecht brechen**, würde es in einem anderen Staat ein „Hack-Back“ anwenden. Das wäre aber sehr wahrscheinlich der Fall, da sich Angriffe über mehrere Staaten erstrecken und nicht nachvollzogen werden kann, woher sie eigentlich kommen. Die Gefahr der Eskalation eines zwischenstaatlichen Konflikts liegt auf der Hand!

Österreich macht sich **mitschuldig an Menschenrechtsverbrechen**. Die NSO-Firma entstammt der Eliteeinheit Unit 8200. Die Software wurde gegen die PalästinenserInnen entwickelt und an ihnen getestet. Entsprechend verkauft NSO die Spyware Pegasus an Staaten, die sie gegen RegimekritikerInnen einsetzen: Marokko, Peru, Usbekistan, die VAR.

Eine kanadische Firma hat nachgewiesen, dass nur über einen whats-up Anruf bei einem Regimekritiker die Überwachungssoftware installiert werden konnte, sogar ohne dass er den Anruf angenommen hat.

Goldman-Sachs und Blackstone haben in diese Firma investiert. Sie hat im Jahr 2018 einen Umsatz von rund 250 Millionen Dollar gemacht.

Israel zeigt sich ganz groß im „**Krieg gegen den Terror**“. Wen es mit „Terroristen“ meint, hat es in den Gaza Kriegen gezeigt und beweist es täglich aufs Neue: Es sind palästinensische ZivilistInnen, Kollateralschäden im Krieg gegen die palästinensischen Fedayin, die ihr im Völkerrecht verbrieftes Recht auf militanten Widerstand gegen die Besatzung wahrnehmen.

Gezielte Kollateralschäden.

Auch die israelische Bevölkerung wird mehr und mehr Adressatin eines völlig aus dem Lot gekommenen Überwachungswahns, wie die Interventionen des israelischen Inlandsgeheimdienstes Shin Bet mit den Corona-Apps zeigten.

Soll Österreich nun ein zweites Israel werden?

Wenn es nach unseren Politikern geht, sieht es danach aus:

Der SP-Politiker Droschitz hat schon 2016 die **Grenzanlagen** im Sinai inspiziert und sich dort Anregungen für die Überwachung der österr. Grenze geholt. Kein Problem für ihn, dass auch die US-mexikanische Grenze mit israelischer Spyware ausgestattet ist und schon tausenden Menschen das Leben gekostet hat. Dass der israelische Sperrwall, der den palästinensischen BäuerInnen weiteren Boden raubte mit dieser Technologie nahezu die gesamte Westbank überwacht.

Die „Terroristen“ sind in Palästina wie Mexiko Menschen, die ein Überleben aus

einem Elend suchen, das von genau jenen verursacht wurde, die sie jetzt von sich fernhalten wollen.

Wir fragen die IT-Krieger, die hinter diesen Mauern ihrem dunklen Handwerk nachgehen:

- Haben Sie jegliches Bekenntnis zu Menschenrecht und Völkerrecht aufgegeben?
 - Ist es Ihnen wirklich gleichgültig, mit welchen Mitteln sie hantieren?
 - Wen Sie damit treffen?
 - Welche Folgen das haben kann?

Ist den Verantwortlichen nicht klar, dass sie die österreichische Bevölkerung völlig an den Big-Data-Schlund der Konzerne wie Apple, Google etc. schleudern, wenn sie mit Programmen israelischer Herkunft arbeiten, die intensivst mit diesen Konzernen vernetzt sind? Sie machen BürgerInnen zu gläsernen Menschen und liefern sie irgendwelchen Profitinteressen aus.

Wissen Sie nicht, dass die Einführung von **Smart Meter** in die österreichische Infrastruktur uns alle höchsten Gefahren aussetzt? Wer die entscheidenden Codes hat, kann sie verkaufen, kann sie erpresserisch nutzen. Welche Software verkauft Frau Kern mit ihren guten Beziehungen nach Israel?

Wer bezahlt im Falle einer Erpressung und/oder eines gezielten Black-Outs? Die österreichische Bevölkerung und es stehen Menschenleben auf dem Spiel.

Sind Sie in diesem Gebäude derartig auf Krieg eingeschworen, dass sie das Offensichtliche nicht sehen, nämlich dass **Sie** einem Staatsterror zuspielen? Ein Terror der im Kleid von Start-ups und Profitversprechen daherkommt? Ein Terror, der Sicherheit verspricht, indem er Unsicherheit schafft? Ein Terror, der mit dem Finger auf andere zeigt, derweil selbst seine unterirdischen Atomanlagen in Bereitschaft hält?

Hören Sie auf sich manipulieren zu lassen!

Denken Sie nicht, dass Sie, wenn Sie mit den israelischen Geheimdiensten arbeiten, eine weiße Weste haben!

Kein Antisemit zu sein, ist etwas ganz anderes als mit der Macht zu heulen, kommt sie nun in blau, türkis, rot oder grün daher.

Steigen Sie aus aus ihrer virtuellen Welt und kommen sie herunter zu uns. Hören Sie die Geschichten der vertriebenen PalästinenserInnen, der syrischen und afghanischen Flüchtlinge, der Muslime und MigrantInnen, die so gern als potentielle TerroristInnen präsentiert werden, um die Bevölkerung aufzuhetzen und kriegskompatibel zu machen.

Wir fordern Sie auf, ihrer eigentlichen Aufgabe, dem Schutz und der Verteidigung des Landes nachzugehen, wie es in der Verfassung steht! Schaffen sie sichere Systeme, Datenschutz auf allen Ebenen und gehen Sie rigoros gegen Datenmissbrauch vor!

Verweigern Sie die Verwendung von Überwachungs- und Kriegstechnologie aus Israel!

Stehen Sie mit Julian Assange, Edward Snowden, Bradley Manning und mit uns ein für Freiheit, Gerechtigkeit und Frieden für alle Völker und Menschen dieser Welt!

Freiheit für Palästina!