Stellungnahme Josef Dittli, per Mail, 9.6.2021

Grundsätzliches:

1. Für mich wirkt der (durchaus interessante) Text etwas polemisch und reisserisch dargestellt.
2. Bei dem geschilderten Szenario handelt es sich nicht um die Beschreibung eines Cyber-Angriffs, sondern um eine Open Source Intelligence (OSINT) Tätigkeit mit anschliessender Sabotage oder dem Versuch einer Abhörung durch «Wire-Tapping». Dabei hat es zwar Cyber Elemente, diese sind jedoch nicht die entscheidenden Elemente.
3. Etwas prägnanter als im dargelegten seitenlangen Text formuliert sagt das Szenario Folgendes aus: Aufgrund eines öffentlich einsehbaren Registers (Netzplan Swisscom) lassen sich Infrastrukturelemente identifizieren (Verteilerkästen / Zuleitungen), welche nachher physikalisch zerstört oder manipuliert werden können. Im Grundsatz kann man mit genügend krimineller Energie einer Firma immer schaden, wenn man deren Infrastruktur oder öffentliche Infrastruktur zerstört (so auch Zufahrtsstrassen, Entladerampen, etc…). Deshalb sind Firmenareale und auch wichtige öffentliche Infrastrukturen entsprechend gesichert. Bei Bundesinfrastrukturen wird meines Wissens neben der Cybersicherheit immer auch die physikalische Sicherheit betrachtet und es werden Risiken ausgewiesen. Das geschilderte Risiko des Verlustes des Zugangs aufgrund eines Wegfallens der Swisscom Leitung wird – sofern als relevantes Risiko identifiziert – durch redundante Zugänge gelöst (z.B. alternative physikalische Leitungen oder Funkverbindungen).
4. Es werden viele Tools und auch Technologien genannt. Diese sind jedoch weder entscheidend und zum Teil auch nicht für den geschilderten Zweck verwendbar (Details unten).
5. Das Szenario ist generell schon möglich, der Schaden aber wesentlich eingegrenzter als im Artikel beschrieben und der Erfolg würde einen sehr hohen Aufwand für relativ wenig Effekt bedeuten.
6. Es war schon früher möglich, anhand von öffentlichen Daten geheime Anlagen zu finden (gut ausgebaute Wege, die im Niemandsland enden, Besuch in den entsprechenden Restaurants in den Bergen …)
7. Das, was der «Experte» zeigt, sind gewöhnliche Angriffsszenarien, die in jedem Penetration Kurs gelehrt und diskutiert werden. **Ich stimme aber mit ihm überein, dass viele Firmen das Thema des Schutzes der internen Kommunikation vernachlässigen und bei E-Mails jegliche Absicherung vermissen lassen.**
8. Die meisten Datendiebstähle, die wir sehen (sowohl kriminell, wie auch staatlich) geschehen aber nicht durch diese Szenarien, sondern via kompromittierte Endgeräte. Es lohnt sich deshalb den Fokus dort zu legen, wo das grösste Risiko ist und dies ist primär bei dem Schutz der Endgeräte, dem schnellen Erkennen von lateralen Bewegungen und von Datenexfiltrationen, da diese sowohl in ihrer Häufigkeit und in ihrem Schadensausmass viel stärker zu gewichten sind, als die erwähnten Szenarien. **Generell ist aber der Einsatz von verschiedenen Verschlüsselungsebenen sehr sinnvoll und sollte - gerade in sensiblen Bereichen - gemacht werden.**

Phase 1: Aufklärung

1. Es wird suggeriert, dass man trotz Anmeldeverfahren seine Identität verschleiern kann. Generell kann man mit genügend Aufwand so etwas machen, es ist jedoch nicht einfach von jedermann ohne Vorwissen durchführbar.
2. Es ist heute nicht mehr einfach, eine unregistrierte Mobilfunknummer zu bekommen. Es gibt meines Wissens zwar Möglichkeiten, zum Teil ausländische Nummern zu

erhalten, welche nicht registriert sind, oder Nummern zu kaufen die auf jemanden anderen registriert sind. Dann muss man jedoch auch die Spuren über den Kauf verwischen. Möglich ja, aber mit Aufwand verbunden.

3. Es werden Tor und VPNs erwähnt, dass man nach quasi anonymer Registrierung nicht zurückverfolgt werden kann. Die genannten Technologien erlauben ein anonymes Surfen im Internet. Das hat Vorteile (z.B. Quellenschutz, Informationsfreiheit) und kann die Ermittlung bei Straftaten erschweren. Allerdings ist zu erwähnen, dass jederzeit ein quasi anonymer Zugang aus Gästenetzwerken (z.B. Hotels, Internet Cafés oder anderen öffentlichen WLANs) möglich ist. Ein Sperren des Zugriffs über diese Anonymisierungstools zu Informationen, welche entsprechend frei verfügbar sind, erscheint mir als nicht zielbringende Massnahme.
4. Die Netzdaten sind gewollt einsehbar. Swisscom verweist korrekterweise auf die Risikoeinschätzung. Ich teile diese. Schliesslich könnte man ja einfach durch die Strasse gehen und würde die Verteilerkästen ja auch sehen, wenn man sie sucht. Und falls man dann physikalisch sabotieren oder zugreifen wollte, müsste man da ja eh hin.
5. Es wird erwähnt, dass plötzlich im Wald endende Leitungen auf klassifizierte Objekte hinweisen können. Generell kann diese Aussage korrekt sein, wenn das Objekt zu nahe am gezeigten Ende wäre und es sichergestellt ist, dass es sich effektiv um klassifizierte Objekte handelt und nicht «normale» ändernde Eigentumsverhältnisse. Zu diesem Fakt müsste man aber das VBS befragen. Generell werden solche Dinge in Informationssicherhits und Datenschutzkonzepten berücksichtigt.

Phase 2: Zugriff / Sabotage

1. Sabotage an Infrastruktur auf öffentlichem Grund ist generell möglich, ausser bei speziell geschützten Infrastrukturen. Ich bin kein Experte in Verteilsystemen, kann jedoch dazu sagen, dass Verteilungen von grob in fein übergehen und Infrastrukturen welche ein grosses Einzugsgebiet betreffen üblicherweise entsprechenden physikalischen Schutz aufweisen sollten. **Hier ist es jedoch so, dass dieser zum Teil verbesserungswürdig ist.**
2. Die Koordination eines Angriffs auf mehrere Ziele wie im Artikel genannt, braucht einige Planung und kriminelle Energie. Auch sind die Ziele wie z.B. der NDB nicht so einfach zu verwunden. Wenn man so viel Energie investiert und Sabotage durch Zerstörung betreiben will, gibt es effektivere und einfachere Möglichkeiten. Das geschilderte Szenario ist zwar durchführbar, hätte aber wahrscheinlich nur einen kleinen Effekt und wäre erst noch eine schwere Straftat, welche die Risiken für die Angreifer kaum im Verhältnis zum Nutzen stehen lassen.
3. Egal ob Sabotage oder Abhörung, der Schaden wäre wesentlich geringer als im Text dargestellt (gutes Beispiel ist Ägypten, wo Aktivisten sich alternative Netzzugänge innert Kürze geschaffen haben, als die Regierung die Verbindungen gekappt hat.)
4. Es ist meines Wissens so, dass gerade Voice over IP Daten meist verschlüsselt sind. Encrypt everything bezieht sich auf alle Daten. Es kann sein, dass gewisse Daten nicht verschlüsselt wären. Diese abzuhören wäre jedoch wesentlich aufwändiger als dargestellt. Die erwähnten Technologien (Raspberry Pi etc…) reichen nicht aus um das zu machen. Sie sind in den genannten Szenarien zu wenig leistungsfähig und könnten lediglich Leitungen mit kleinen Datenmengen leicht abhören. (Ausserdem: Warum soll ich eine Batterie verwenden, wenn ich eh an den Verteilerkasten gehe. Da hat es Strom drin).

Abschliessende Gedanken: Ich zweifle etwas an der Expertise der Experten, da sie eher grundlegende Gedankenspiele durchspielen. Diese machen sich Einsteiger in die Materie oder Laien. Experten verstehen, dass die Details komplexer sind und würde ein Szenario entsprechend detaillierter und weniger «reisserisch» darstellen. Das soll aber nicht heissen, dass der Schutz von kritischen Infrastrukturen in vielen Fällen nicht noch verbessert werden kann.