Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 183 (2017)

Heft: 9

Artikel: Sicherheit von morgen beginnt mit Nachrichtendienst und Cyber-Abwehr

Autor: Maudet, Pierre

DOI: https://doi.org/10.5169/seals-730693

Sicherheit von morgen beginnt mit Nachrichtendienst und Cyber-Abwehr

Der Schutz der Grenzen beschränkt sich heute nicht mehr auf die üblichen Übergangsstellen, welche bisher durch den Zoll und das Grenzwachtkorps bewacht wurden. Der Schutz der Grenzen geht weit darüber hinaus. Mit der «Grünen» Grenze kennen wir seit langem eine weitere Kategorie. Nur mit genügend technischen und personellen Mitteln lässt sich letztere zuverlässig überwachen. Neu kommt allerdings mit der «Grauen» Grenze eine digitale Form im Bereich der Informationsbeschaffung und der Cyber-Abwehr hinzu, welche uns vor grosse Herausforderungen stellt.

Pierre Maudet

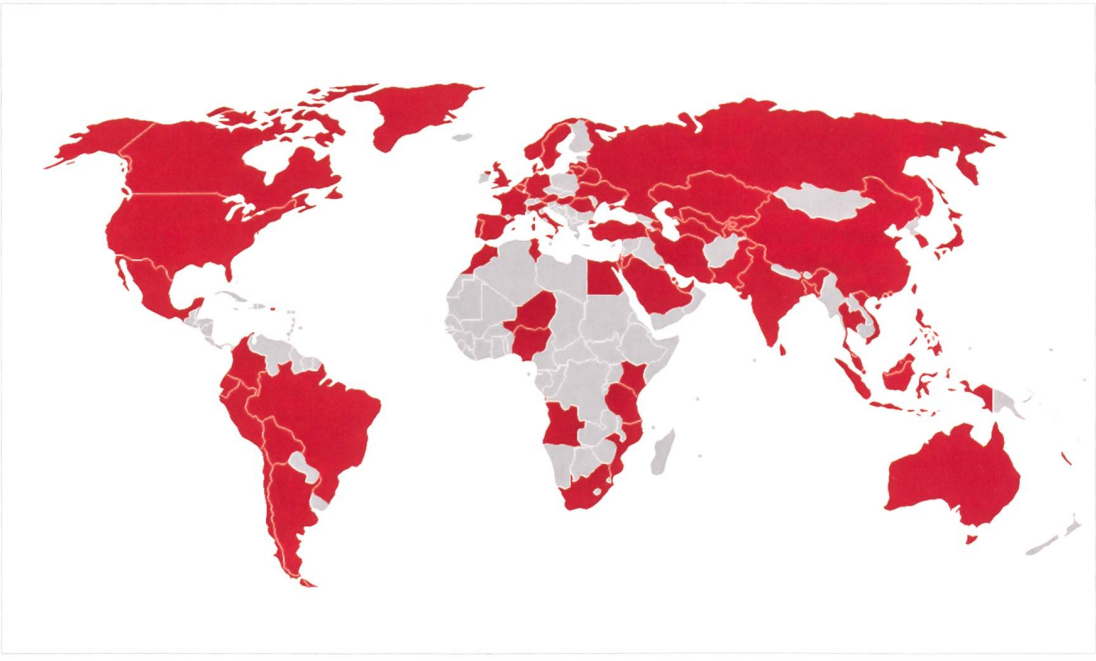
Das Nachrichtendienstgesetz, welches mit einem Ja-Stimmenanteil von 65,5% am 25. September 2016 angenommen wurde, spricht hier für die Einsicht der Schweizer Bevölkerung. Der Nachrichtendienst ist unsere erste Verteidigungslinie.

Vorausschauen

Ohne gezielte Informationen, ohne Antizipation und ohne Vernetzung, bleibt jede Aktion rein reaktiv – damit ist sie oft zu spät und ineffizient. Wie in der Armee sind Feuer und Bewegung unwirksam ohne gute Zielaufklärung, ohne ein gezieltes Feuer und ohne genaue und wendige Pläne. Es ist heute entscheidend, zu antizipieren und vorauszudenken. Das gilt ebenso in der Wirtschaft wie auch in Energie-, Klima-, Technologie- und Verkehrs- oder auch bei Fragen zur Kriminalität.

«Es ist heute entscheidend, zu antizipieren und vorauszudenken.»

Wir verfügen über neue juristische Mittel im Bereich des Nachrichtendienstes, welche noch dieses Jahr in Kraft treten. Aber wir dürfen da nicht aufhören. Unser Strafmass für Dschihadreisende oder für solche, welche kriminelle oder terroristische Organisationen unterstützen, gehören zu den schwächsten ganz Europas. Einige vorgeschlagene Massnahmen und Kontrollmittel sind eher symbolischer Natur – wenn nicht sogar reine Folklore – als denn wirklich effizient. Die Schweiz darf nicht zum weichen Unterleib Europas werden. Die Realitätsverweigerung muss aufhören. Die Rechte der Kriminellen sollen nicht die Rechte der potentiellen Opfer schmälern. In einem Rechtsstaat dürfen rechtsstaatliche Prinzipien keinesfalls zur Hypothek für die Sicherheit der Bevölkerung werden. Es liegt in der Verantwortung der Regierung, daran zu erinnern, dass mit Rechten auch Pflichten einhergehen.



Vom «WannaCry»-Virus betroffene Länder (Mai 2017).

Schützen

Vor einigen Jahren redete man noch von IT-Sicherheit bildlich in Form eines «virtuellen Tresors». Es handelte sich dabei um den Bau von Firewalls rund um den Server. Diese Strategie beruhte damals exklusiv darauf, sensible Daten zu isolieren und voneinander zu separieren. Im Jahr 2014 wurden weltweit rund 2,5 Milliarden Dollar in IT-Sicherheit

Screenshot eines vom «WannaCry-Virus» betroffenen Rechners. Bilder: Wikipedia

investiert. Im Jahr 2020 werden diese Kosten wohl voraussichtlich bereits 155 Milliarden Dollar betragen.

Heute reicht ein ausschliesslich defensives und reaktives Vorgehen schlicht nicht mehr aus. Mehr denn je sind Unternehmen oder kritische Infrastrukturen in ganz Europa Ziel von Cyber-Attacken und von Ransomware (aus dem Englischen ransom für Lösegeld). Dieses Jahr haben verschiedene Angriffswellen Schweizer Unternehmen getroffen: Innert weniger Sekunden haben betroffene Firmen rund drei Prozent ihres jährlichen Umsatzes verloren. Dies mal ganz abgesehen vom Vertrauens- und Imageverlust. Die Verwaltung, aber auch kritische Infrastrukturen wie Spitäler sind genauso davon betroffen.

Wir brauchen eine zielgerichtete Politik, was die Cyber-Abwehr betrifft. Sie sollte sich auf mehrere Elemente stützen:

- Die Verfolgung technologischer Entwicklungen und eine gezielte Förderung der Forschung. um unsere Kenntnisse zu erweitern und zu integrieren, aber auch um die Branche der IT-Sicherheit in der Schweiz zu fördern. Dieser Wachstumsbranche geht es gut und sie kann zu einem wesentlichen Erfolgsfaktor für die wirtschaftliche Entwicklung der Schweiz in den nächsten Jahren werden, indem sie zahlreiche hochqualifizierte Arbeitsplätze schafft;
- Eine fundierte Grundausbildung zum Thema IT-Sicherheit an unseren Schulen, in den Unternehmen und in der Verwaltung mit einfachen und klaren Botschaften – gemäss der bekannten Maxime von «schweigen – einschliessen – tarnen»;
- Die Kantone und vor allem der Bund stellen das Know-how, die Mittel und die Infrastruktur bereit, um unsere Unternehmen zu beraten und ihnen helfen zu können. Diese typisch schweizerische Form der Zusammenarbeit funktioniert gut;
- Schliesslich – im Falle eines direkten Angriffes auf die Wirtschaft, die kritische Infrastruktur des Landes und unsere strategischen Interessen – muss der Bund ebenfalls über die nötigen Mittel verfügen, darauf eine effiziente Antwort geben zu können.

«Es liegt an uns, die strategischen Sicherheitsinteressen des Landes konkret zu definieren, um Risiken vorauszusehen ... »

Verteidigen

Die Änderungen, von denen wir reden, lassen sich nicht mit dem Kauf von EDV-Ausstattung, dem Einstellen von Spezialisten oder der Unterstützung einzelner Projekte zusammenfassen. Wir müssen uns mit dem Nachrichtenwesen, der Sicherheit und strategischen Fragestellungen ernsthaft auseinandersetzen. Es liegt an uns, die strategischen Sicherheitsinteressen des Landes konkret zu definieren, um Risiken voraus zu sehen, die nötigen Mittel bereit zu stellen und die Sicherheit der Schweiz, seiner Bevölkerung, seiner Wirtschaft, seiner strategischen Interessen – nicht nur seiner Grenzen und des Territoriums – weiterhin und uneingeschränkt garantieren zu können.

Städte und Terrorismus

Ist der Terrorismus nur ein vorübergehendes Phänomen oder eine andauernde und bleibende Bedrohung? Obwohl er tief in der Geschichte verankert ist, müssen wir uns weder an ihn gewöhnen, noch akzeptieren und ihn sicherlich nicht rechtfertigen. Der Terrorismus ist insofern einzigartig, da er jedes Glied unser Sicherheitskette unter Druck setzt – vom Nachrichtendienst über die Gesetzgebung, unsere Polizeikräfte, die Regierung, alle sicherheitsrelevanten Entscheidungen, bis hin zu unserem Strafvollzugssystem. Allgemeiner betrachtet, setzt der Terrorismus unsere Gesellschaft, unseren Zusammenhalt, unsere Werte nachhaltig unter Druck.

Die Schweiz ist keine Insel. Auch sie ist mit vergleichbaren Problemen und oft den gleichen Risiken wie unsere Nachbarn konfrontiert. Um den Terrorismus zu bekämpfen, um die Kriminalität und die unkontrollierte Migration, den Klimawandel oder technologische Risiken zu meistern, ist eine eingespielte Zusammenarbeit entscheidend. Doch wer kooperieren will, muss auch eigene Mittel, Kapazitäten, Know-how, Kompetenz und Erfahrungen einbringen – denn nur dann wird eine echte partnerschaftliche Kooperation funktionieren. ■

Hauptmann
Pierre Maudet
Master Rechtswissenschaft
Regierungsrat FDP
Vorsteher Sicherheitsdep.
1200 Genf