Teile und herrsche: Cyber-Sicherheit durch Fusionszentren

Effektive Cyber-Abwehr erfordert die Kombination relevanter Information aus einer Vielzahl von Quellen und Organisationen. Fusionszentren sind eine öffentlich-private Organisationsform, in der diese Kombination stattfindet. Das Ziel ist die Schaffung eines komplexen Lagebildes, das eine schnellere und präzisere Cyber-Abwehr ermöglicht.

Marcus M. Keupp, Dimitri Percia David, Alain Mermoud

Unser letzter Artikel in der ASMZ 07/2018 präsentierte einige Erkenntnisse, wie und warum die Cyber-Sicherheit durch Informationsaustausch in *Information Sharing and Analysis Centers (ISACs)* verbessert wird. In diesem Artikel dehnen wir unsere Betrachtungen auf Fusionszentren *(fusion centers)* aus.

Das Teilen sicherheitsrelevanter Informationen innerhalb von ISACs hat den Nachteil, dass pro Transaktion nur ein diskreter Informationswert geteilt wird. Die für eine effektive Cyber-Abwehr komplexer Bedrohungen notwendige Information ist zudem zwischen vielen Organisationen und Akteuren fragmentiert, sodass die Gewinnung eines vollständigen Lagebildes teuer ist oder lange dauert. Trotz umfassender Aufklärungsbemühungen kommt daher ein nur unvollständiges Lagebild zustande. Abbildung 1 illustriert schematisch diese Problematik.

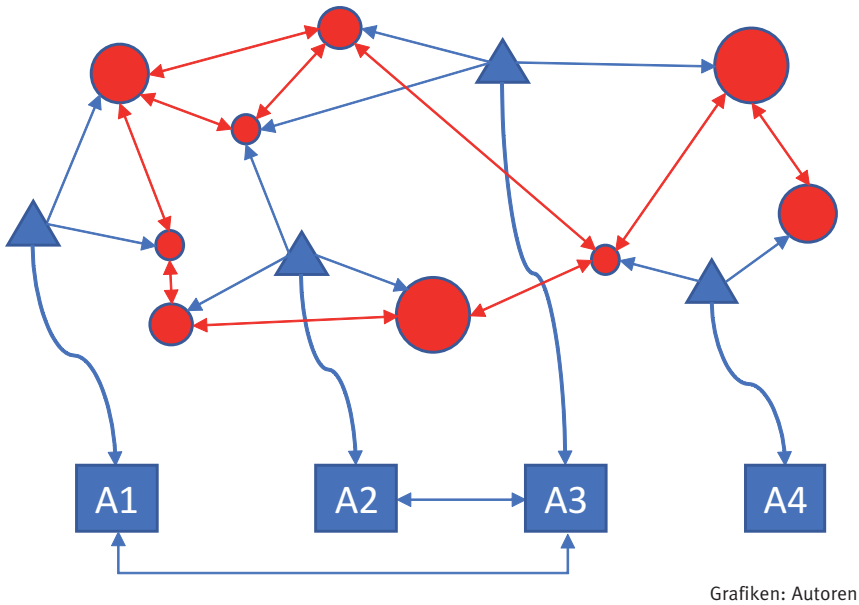
Die Akteure A1 bis A4 haben jeweils einen Sensor in einer hybriden gegnerischen Struktur etabliert. Jede dieser Quellen liefert Information zugunsten jedes einzelnen Akteurs. Obwohl jedes gegnerische Strukturelement von mindestens einer Quelle beobachtet wird, besitzt kein einzelner Akteur ein korrektes oder auch nur vollständiges Lagebild. Im Gegenteil erhält er nur fragmentierte Information, die die gegnerische Struktur unzureichend beschreibt. Erschwerend kommt hinzu, dass die Akteure ihre fragmentierte Information nicht unbedingt miteinander teilen. Der Akteur 3 tauscht zwar Information mit den Akteuren 1 und 2, nicht jedoch mit Akteur 4 aus. Akteur 1 spricht nicht mit Akteur 2, und Akteur 4 teilt überhaupt keine Informationen. Diese Fragmentierung der Nachrichtenlage macht eine Entschlussfassung daher riskant, wenn nicht gar unmöglich.

Die Idee eines Fusionszentrums ist es, diese Fragmentierung durch die Integration der Informationen aller Akteure zu beenden. Abbildung 2 illustriert den angestrebten Zustand. Alle Akteure speisen ihre individuell gewonnenen Erkenntnisse in das Fusionszentrum ein. Durch Verknüpfung der einzelnen Informationen ist es nun möglich, ein vollständiges Lagebild zu erstellen und zielführende Entschlüsse zu fassen.

Fusionszentren – de quoi s'agit-il?

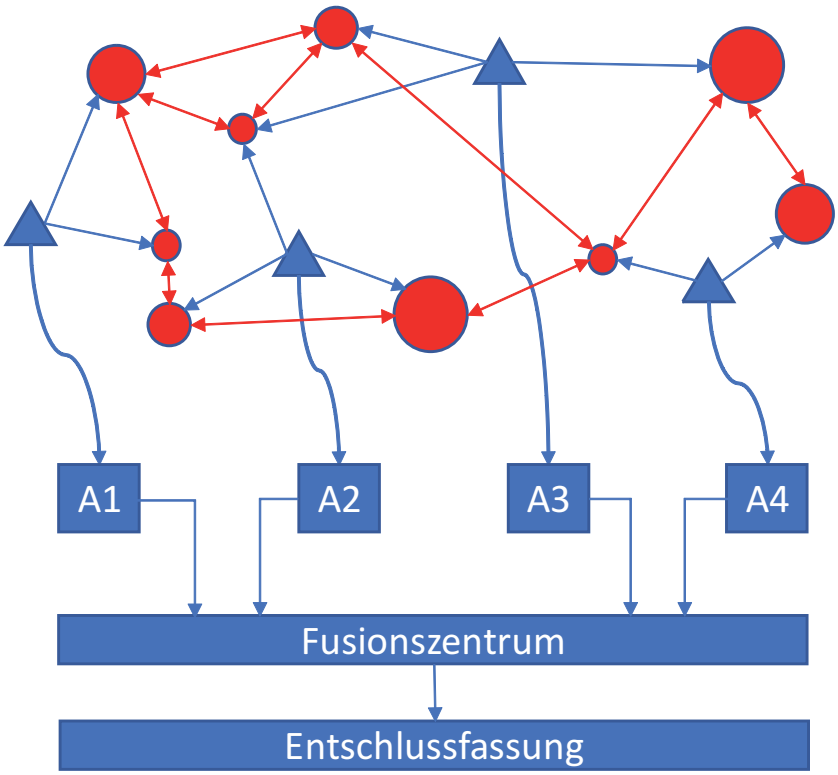
Fusionszentren (fusion centers) sind physische und/oder virtuelle Räume, in denen eine Zusammenarbeit zwischen verschiedenen Akteuren des öffentlichen und privaten Sektors zu einer Kombination von Cyber-Fachwissen aus vielen Quellen führt. Fusionszentren versuchen, Informationen aus verschiedenen Quellen aufzubereiten und themengerecht zu bündeln. Sowohl staatliche Strafverfolgungsbehörden (auf nationaler und regionaler Ebene) als auch Akteure des privaten Sektors teilen wechselseitig – idealerweise in Echtzeit – ihre Informationen, um präzisere und robustere Analysen zu generieren. Die so gewonnenen Erkenntnisse ermöglichen es, Cyber-Angriffe schneller zu erkennen und zu bekämpfen. Aktuelle Beispiele sind das *Kudelski Cyber Fusion Center* (https://www.kudelskisecurity.com/services/managed-security) sowie die Fusionszentren der *National Fusion Center Association* in den USA (https://nfcausa.org/). Im Verteidigungsbereich betreibt die NATO seit 2007 das *Intelligence Fusion Center,* wenngleich bei der Gründung noch nicht die Cyber-Sicherheit, sondern der internationale Terrorismus im Fokus der Analyse stand.

Abbildung 1



Grafiken: Autoren

Abbildung 2



Das US-amerikanische Beispiel: ein öffentlich-privates Quellennetzwerk

In den USA wird dieser Vernetzungsprozess seit 2003 durch das *Department of Homeland Security* vorangetrieben. Auslöser dieser Entwicklung war die Erkenntnis, dass die verschiedenen US-amerikanischen Sicherheitsbehörden im Jahr 2001 zusammengenommen über ausreichende Informationen verfügten, um die Terroranschläge des 11. September 2001 zu verhindern, ihre isolierten Informationen aber nicht zu einem komplexen Lagebild kombinieren konnten. Die heutigen Fusionszentren verknüpfen daher Information von Geheimdiensten (NSA, CIA, FBI), Bundesbehörden (DEA, TSA, Nationalgarde) und privaten Akteuren (Google, Apple, Facebook, Amazon, Microsoft). Die Zusammenarbeit ist föderal organisiert; jeder US-Bundesstaat betreibt ein eigenes Fusionszentrum. Zusammengenommen bilden diese ein nationales Netzwerk von Nachrichtenquellen. Bereits im Jahr 2014 hatten 63 von 78 Fusionszentren eine *cyber mission,* das heisst den Auftrag, ein Lagebild über Cyber-Angriffe und deren Abwehrmöglichkeiten zu erstellen.

«Die Schweiz verfügt über eine Vielzahl nachrichtendienstlicher Akteure und wettbewerbsfähiger IT-Unternehmen, sodass die Gründung von Fusionszentren attraktiv erscheint.»

Möglichkeiten für Schweizer Fusionszentren

Ein aktuelle Studie beleuchtet die Austauschbeziehungen zwischen verschiedenen Akteuren der schweizerischen Sicherheitspolitik.* Zwar ist eine gewisse Vernetzung zu erkennen, allerdings besteht immer noch eine erhebliche Fragmentierung. Die Schweiz verfügt über eine Vielzahl nachrichtendienstlicher Akteure und wettbewerbsfähiger IT-Unternehmen, sodass die Gründung von Fusionszentren attraktiv erscheint. Der föderalistische Staatsaufbau erweist sich hier als vorteilhaft, weil die einzelnen Fusionszentren analog zum US-amerikanischen Beispiel auf der kantonalen Ebene gegründet werden könnten.

Die Probleme der Umsetzung stellen sich vielmehr aus politökonomischer und rechtsstaatlicher Sicht. Einerseits hat nicht jeder Akteur, der Information besitzt, auch ein Interesse daran, diese zu teilen. Im Gegenteil besitzt Information gerade im nachrichtendienstlichen Bereich den Charakter einer Handelsware. Daher müssen nicht nur Organisationen, sondern auch zielführende Interaktionsregeln geschaffen werden, die den Akteuren einen Anreiz zum freiwilligen Austausch von Informationen geben. Andererseits untersteht zwar die individuelle Nachrichtengewinnung den Schranken des Rechtsstaats und gegebenenfalls einer parlamentarischen Aufsicht, nicht jedoch deren Verknüpfung. Wer in der Lage ist, viele Informationen dezentraler Akteure zu komplexen Lagebildern zu verknüpfen, wird selbst ein mächtiger Akteur. Dies gilt insbesondere dann, wenn das Fusionszentrum von privaten Firmen betrieben werden sollte, die auch kommerzielle Interessen verfolgen. Es reicht in einem entwickelten Rechtsstaat freiheitlicher Prägung daher nicht aus, nach digitaler Souveränität zu rufen, wenn der Weg dorthin in die totalitäre Überwachung führt. Die Cyber-Verteidigung der Zukunft wird daher einer politischen und fachlichen Aufsicht bedürfen, wie sie heute bereits bei den staatlichen Nachrichtendiensten besteht. ■

* Hagmann, J., Davidshofer, S., Tawfik, A., Wenger, A., Wildi, L. 2018. The Programmatic and Institutional (Re-)Configuration of the Swiss National Security Field. Swiss Political Science Review. doi:10.1111/spsr.12304


Marcus M. Keupp
PD Dr. oec. HSG
Dozent Militärökonomie
MILAK
8903 Birmensdorf ZH


Hptm
Dimitri Percia David
Msc
Wissenschaftlicher
Mitarbeiter der MILAK
8903 Birmensdorf ZH


Hptm
Alain Mermoud
Msc
Wissenschaftlicher
Mitarbeiter der MILAK
8903 Birmensdorf ZH