Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 187 (2021)

Heft: 9

Artikel: Multidomain nach Schweizer Art : smart und vernetzt

Autor: Vögeli, Urs

DOI: https://doi.org/10.5169/seals-976273

Multidomain nach Schweizer Art: smart und vernetzt

In jüngerer Vergangenheit hat der Begriff Multidomain zu inhaltlichen Verwirrungen und konzeptionellen Verwechslungen geführt und auch in der ASMZ für Wirbel gesorgt. Dies hat mitunter damit zu tun, dass dieses Konzept einerseits in der Schweizer Sicherheitspolitik noch relativ neu ist und andererseits im internationalen Kontext fast schon inflationär verwendet wurde. Als Milizoffizier und Abonnent der ASMZ möchte ich hierzu mit einem klärenden Beitrag die Debatte anreichern und anregen.

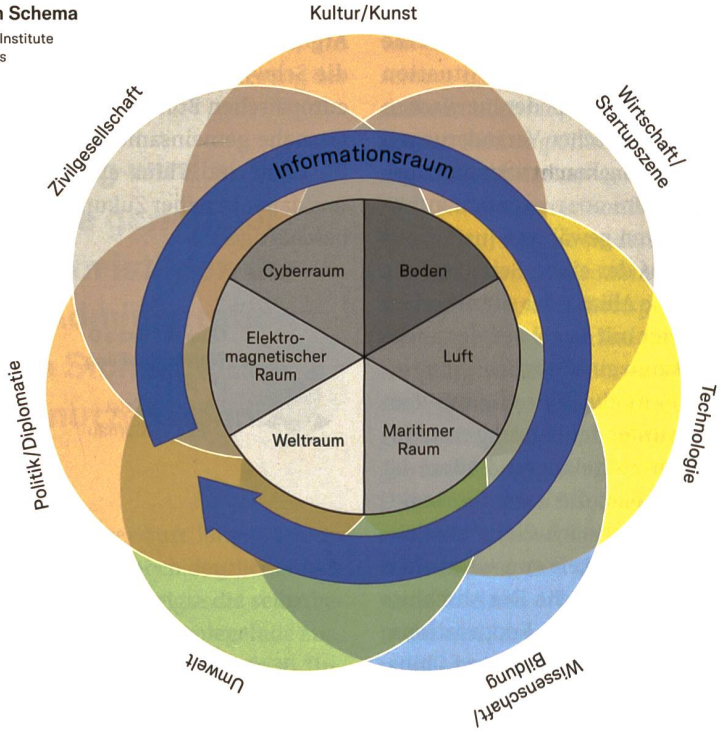
Urs Vögeli

Der Begriff Multidomain ist stark von rüstungs- und marketingtechnischen Referenzen angetrieben, gerade im Kontext einer amerikanisch geprägten Definition. Multidomain ist im US-amerikanischen Kontext eine Neuauflage des *Joint-Gedankens* (Führung des Einsatzes der Mittel im Verbund), eine Reinkarnation der Idee der vernetzten Kriegsführung (Network Centric Warfare) und ein Versuch, die eher neuen Operationsdomänen Cyber und Weltraum proaktiver zu integrieren. Im Kontrast zum amerikanischen Modell ist die chinesische Variante von der Idee der informationsgetriebenen Kriegsführung durchdrungen und geht dabei noch einen Schritt weiter. Der Informationsraum wird nicht nur technisch verstanden, sondern es geht den Chinesen auch um umfassende Kommunikation im Sinn von Verständigung durch Verwendung von Zeichen und Sprache. Beispielhaft zeigt sich dies in der Schaffung der *Strategic Support Force* (SSF) der Volksbefreiungsarmee Chinas. Dabei wurden nicht nur die Bereiche Weltraum, Cyber und elektronische Kriegsführung zusammengelegt, sondern auch der strategische Nachrichtendienst und psychologische Operationen. Diese Verbindung ist Ausdruck einer Kriegsführungslogik, die politische, rechtliche und mediale Massnahmen miteinschliesst. Gleichsam wurde die SSF im Rahmen von grossangelegten organisationskulturellen Reformen geschaffen, die die Streitkräfte in den Kontext einer grösseren, geostrategischen Agenda der Kommunistischen Partei Chinas stellen.

Mehr als Technologie und Struktur – Multidomainkultur!

Diese Gedanken haben beim Swiss Institute for Global Affairs (SIGA) dazu geführt, den Begriff Multidomain in einen grösseren Kontext zu stellen. Dieser Rahmen soll vornehmlich die rein technologisch und streitkräftebezogene Perspektive erweitern sowie einen Bogen zur Schweiz und ihren politischen und soziokulturellen Eigenarten schlagen. Diese inhaltlichen Erweiterungen basieren auf zwei weiteren Erkenntnissen: Unternehmerische und sozioökonomische Trends entsprechen bereits heute dem vernetzten Multidomain-Denken und gehen in eine ähnliche Rich-

Multidomain Schema
Grafiken: Swiss Institute for Global Affairs



tung. Im Innovationskontext und in der Startup-Szene entstehen aktuell laufend neue Konzepte und Ideen, die ebenfalls nach neuen Kollaborations- und Vernetzungsformen suchen, so etwa das Coworking oder ökosystem- und communitybasierte Geschäfts- und Organisationsmodelle. Es zeichnet sich ab, dass digitale Transformation, Globalisierung, Individualisierung, New Work und weitere Herausforderungen nicht mehr mit herkömmlichen Methoden und Strukturen gemeistert werden können. Insbesondere im Bereich Digitalisierung macht sich zudem die Erkenntnis breit, dass zu lange einseitig technologische Aspekte im Vordergrund standen und jetzt die Zeit der interdisziplinären und menschbezogenen Auseinandersetzung mit Technologie gekommen ist.

Drei Ebenen von Multidomain

Wir schlagen vor, den Begriff Multidomain auf drei Ebenen zu betrachten. Auf der militärisch-operativen Ebene gehört das Konzept Multidomain in die Joint-Familie. Mit Blick auf die chinesische Streitkräfteentwicklungen würden wir von einer klaren Weiterentwicklung der vernetzten Kriegsführung sprechen. Die Verknüpfung von Cyber, Weltraum, Nachrichtendienst und psychologische Kriegsführung, wie es die Chinesen vormachen, stellt westliche Streitkräfte mit ihrem demokratisch-rechtsstaatlichen Kontext jedoch vor Herausforderungen. Wir müssen aber diese neuen Formen von Informationskriegführung und Verbunddenken verstehen, um adäquate Antworten darauf zu finden, die eigene Resilienz zu stärken und die Robustheit unserer Gesellschaft und Institutionen zu gewährleisten. Selbes gilt auch für die geostrategische Ebene. Dem Trend, dass Grossmächte ihre Konflikte zunehmend ganzheitlich, das heisst mit Rückgriff auf Wirtschafts-, Finanz- und Handelspolitik, Diplomatie in internationalen Organisationen, Geschichtsdeutung, Recht, Technologie- und Wissenschaftspolitik austragen, kann ein hochvernetzter und neutraler Kleinstaat Schweiz nur mit smarten und langfristigen Lösungen beikommen. Der grosse Hebel liegt dabei eben gerade auf dem dritten Layer! Wir sprechen von einer organisationskulturellen Ebene. Dabei geht es darum, die Kultur in unseren Sicherheitsarchitekturen auf eine umfassend verstandene Vernetzungs- und Kollaborationskultur auszurichten. Im Gegensatz zum Gesamtverteidigungskonzept funktioniert dieser Ansatz bottom-up und relational. Dabei müssen wir gar nicht so sehr auf die Chinesen oder Amerikaner schauen, sondern können uns unsere Wissenschafts-, Innovations-, Kreativ- und Startup-Szenen zu Nutze machen, indem wir von ihnen lernen, explizit Kontakte zu diesen Ecosphären aufbauen und entsprechend für die sicherheitspolitische Resilienz adaptieren. Diese Szenen haben es verstanden, wie digitale Transformation, Unternehmertum und gesellschaftliches Engagement verbunden werden kann. Interdisziplinäre und auch unkonventionelle Netzwerke, sowie Partizipation und Dialog spielen in diesem Kontext eine grosse Rolle als Katalysator. Dabei ist unsere Milizkultur ein zentrales Schlüsselelement, die genau diese Form von Verbindung gewährleisten könnte. Dabei sollten wir auch an unsere auf Bürgerengagement beruhende Partizipation und dezentralen Strukturen anknüpfen. Dazu zählt ebenfalls unsere breit diversifizierte, global ausgerichtete und kleingliedrige Wirtschaftsstruktur. Der Milizgedanke könnte somit eine Renaissance erleben und kann zentral bleiben zur relationalen Bindungsverstärkung von Gesellschaft, Wirtschaft und Kultur, insbesondere aufgrund der gesteigerten Bedeutung einer getragenen Sicherheitspolitik innerhalb unseres Kleinstaates im Sinne des Multidomain-Gedankens. Über alle Ebenen hinweg – streitkräfteintern, innerhalb der Verwaltung, innerhalb des Sicherheitsverbundes, zusammen mit Wirtschaft und Industrie, aber gerade auch mit der vielfältigen Zivilgesellschaft, mit unserer Sprachenvielfalt, mit Kultur und Kunst, mit Wissenschaft und Bildung – kann der domänenübergreifende Ansatz eine innovative Antwort auf lokale und globale Herausforderungen sein.

Wenn wir in der Schweiz diesen Teil von Multidomain wieder verstehen und bewusst anstreben, was keine zusätzlichen Millionenbudgets verschlingt, werden wir als kleine, aber hochvernetzte Gesellschaft nicht nur für moderne Bedrohungen und Risiken gewappnet sein, sondern auch die digitale Transformation und die sich anbahnenden geopolitischen Erschütterungen meistern. ■

Major Urs Vögeli
MA in Politikwissenschaft
und Geografie
Swiss Institute for Global Affairs
4800 Zofingen
www.globalaffairs.ch

CYBER OBSERVER

Marc Ruef
Head of Research
scip AG

Das Jahr 2021 führt weiter, was im digitalen Zeitalter zur Tradition geworden ist: Gestohlene Daten werden gehandelt und öffentlich gemacht. In der ASMZ-Ausgabe 6/2021 spreche ich vom «Zeitalter der Leaks». In diesem Zusammenhang ist aber neu, dass scheinbar auf der Basis solcher Daten in der Schweiz aktiv Abstimmungskampf betrieben wurde. Personen wurden per SMS angeschrieben, wie die Medien im Juni berichtet haben.

Es ist davon auszugehen, dass in diesem Zusammenhang die Handynummern des Facebook-Leaks hergehalten haben. Diese stammen aus dem Jahr 2019, wurden aber erst zu Beginn des laufenden Jahres an die Öffentlichkeit getragen. Datenschützer waren alles andere als erfreut. Doch handelt es sich bei öffentlich gemachten Leaks wirklich um geschützte Daten? Sind diese mit ihrer Publikation nicht zu allgemein zugänglichen Informationen geworden?

Juristen streiten sich, wie der Sachverhalt nun genau auszulegen ist. DSG Art. 4 erwartet eigentlich eine rechtmässige Bearbeitung, unter Angabe des Zwecks bei der Beschaffung und setzt eine Einwilligung voraus.

Solange dem widersprechende Praktiken nicht konkret geahndet werden, müssen wir auch in Zukunft damit rechnen, dass geleakte Daten unverhohlen zweckentfremdet werden. Die EU-Datenschutz-Grundverordnung DSGVO setzt da im Gegensatz zur Gesetzgebung in der Schweiz drakonische Strafen an. Diese sind erforderlich und müssen durchgesetzt werden. Sonst bleibt der Datenschutz ein Papier ohne Wirkung.

Der mit den vielen Leaks einhergehende virtuelle Schmerz wird hoffentlich dazu führen, dass der öffentliche Druck zunimmt, so dass Organisationen mit laxem Umgang von persönlichen Daten einen Teil des Schmerzes zurückerhalten.