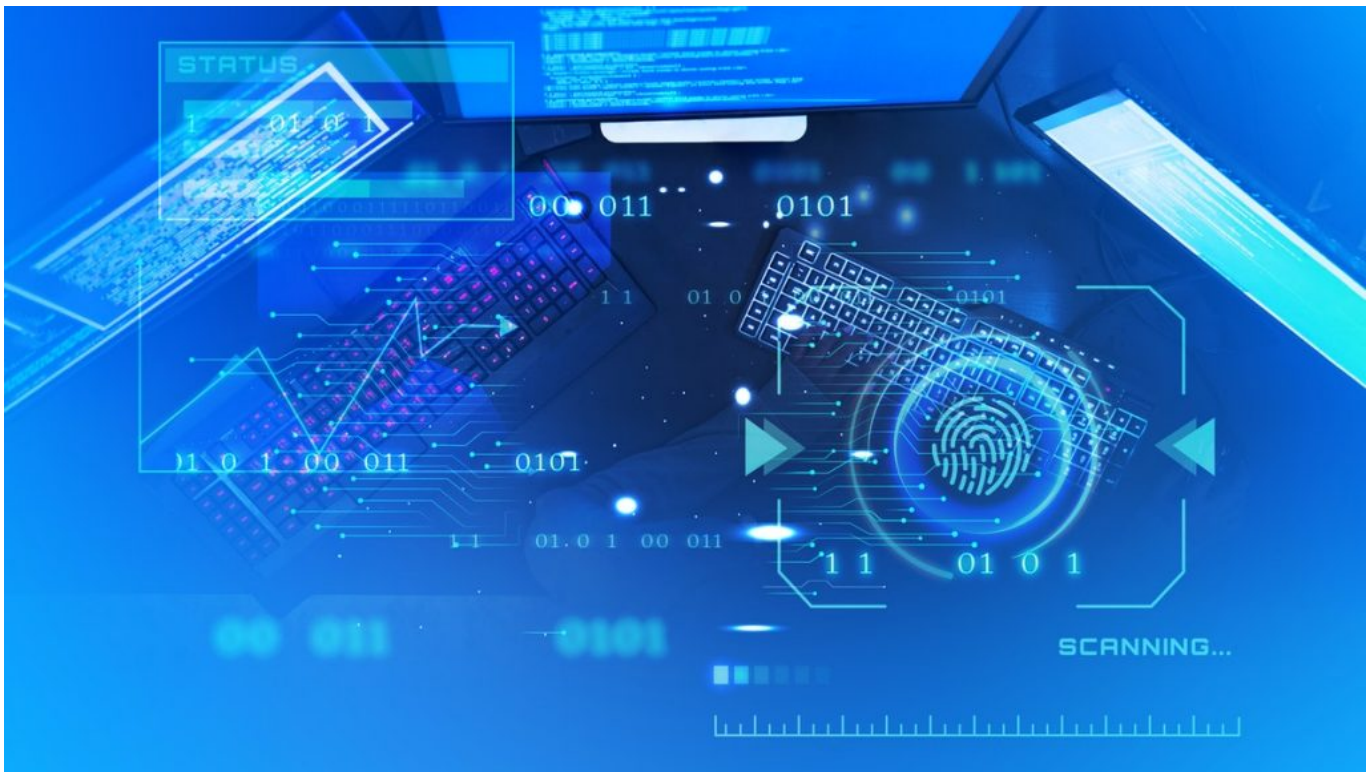
Die Spannungsfelder der Cybersicherheit

Myriam Dunn Cavelty, Florian J. Egloff
18th August 2020



Seit 1. Juli 2020 hat die Schweiz ein Nationales Zentrum für Cybersicherheit (NCSC). Ist dies das Ende des bürokratischen Hickhacks um klare Zuständigkeiten oder vielmehr eine typisch schweizerische Lösung, die vor allem auf dezentrale Strukturen und viel Koordination setzt? Wir zeigen in diesem Beitrag, warum Cybersicherheit genau so und nicht anders angegangen werden muss, es aber auch in Zukunft viel politische Klärung braucht.

Die Cybersicherheit ist in den letzten zehn Jahren von einem technischen Nischenthema zu einem sicherheitspolitischen Dauerthema geworden. Grund dafür ist unter anderem der markante Anstieg staatlicher, strategisch motivierter Aktivität im Cyberraum, die als Begleiterscheinung gegenwärtiger, geopolitischer Anspannungen zu Tage tritt.

Nationale Sicherheitsthemen schaffen es aufgrund der ihnen anhaftenden „Dringlichkeit“ häufig, andere Themen zu verdrängen oder zumindest den Anschein zu erwecken, dass sie nur mit ausserordentlichen, sogar undemokratischen Massnahmen bewältigt werden können. Auch bei der Cybersicherheit gibt es diese Tendenz. Dabei ist sie bei weitem nicht nur eine nationale Sicherheitsproblematik: Cybersicherheit offenbart sich vielmehr als ein typisches Querschnittsthema, bei dem Lösungen nicht ohne Kooperation zwischen unterschiedlichen Akteuren erarbeitet werden können.

Es gilt als weltweit anerkannte Maxime, dass ein zufriedenstellendes Niveau

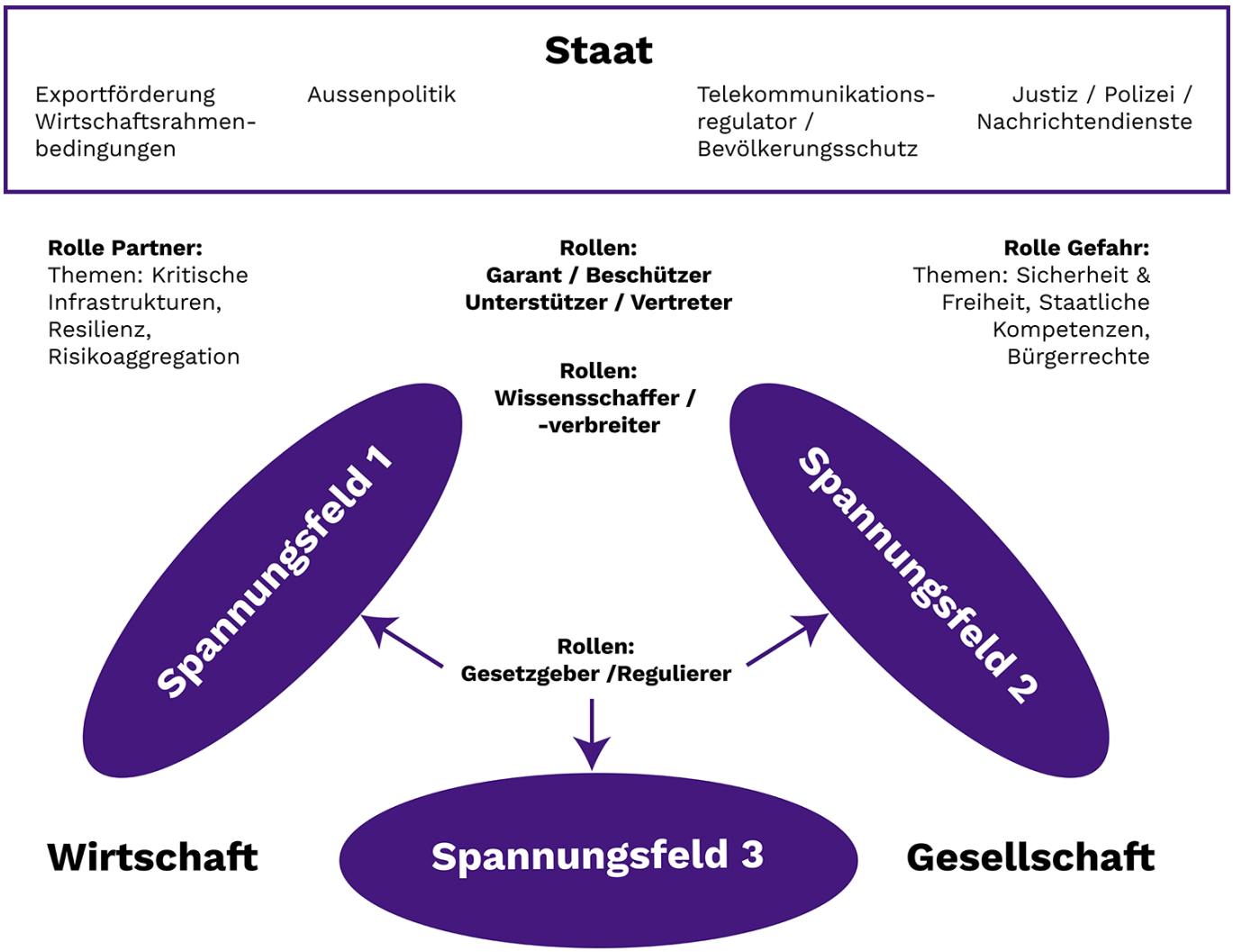
an Cybersicherheit nur im Verbund zwischen staatlichen Stellen, Wirtschaft und Gesellschaft erreicht werden kann. Das macht Cybersicherheitspolitik zu einem Politikfeld, in dem die unterschiedlichen Interessen verstanden und bewusst ausbalanciert werden müssen – wie das im Nationalen Zentrum für Cybersicherheit (NCSC) zumindest angedacht ist. Das heisst aber auch, dass das Schaffen von Strukturen lange nicht genügt. Cybersicherheitspolitik entsteht als Resultat komplexer und dynamischer Aushandlungsprozesse in drei Spannungsfeldern, die bisher zu wenig Beachtung finden.

Die drei Spannungsfelder der Cybersicherheitspolitik

Im ersten Spannungsfeld zwischen Staat und Wirtschaft gilt es, eine Politik zu formulieren, welche die negativen Konsequenzen der Liberalisierung, Privatisierung und Globalisierung aus Sicht der Sicherheitspolitik auffängt, ohne die positiven Effekte zu verhindern. Bei den negativen Konsequenzen geht es zum Beispiel um Themen wie gesellschaftlich sub-obtimale Investitionsentscheide von (in privater Hand gehaltene) kritischen Infrastrukturen oder um sektorübergreifenden Risikoaggregationen bzw. Contagion-Effekte die sich aufgrund der autonomen Entscheide privater Akteure bilden. Dabei geht es dem Staat in diesem Spannungsfeld um die nationale Sicherheit, inklusive der Widerstandsfähigkeit des Gesamtsystems Gesellschaft, zu garantieren.

Im zweiten Spannungsfeld zwischen Staat und Bürger gilt es, die politisch gewünschte Balance zwischen mehr Sicherheit und Freiheit im digitalen Raum zu finden. Zusätzlich geforderte polizeiliche oder geheimdienstliche Befugnisse geraten dabei häufig in Konflikt mit Bürgerrechten, insbesondere dem Grundrecht auf informationelle Selbstbestimmung oder der Anonymität im Netz. Es wird gerne darüber hinweggesehen, dass trotz der erhöhten Aufmerksamkeit und dem Ruf nach mehr und besserem Schutz, die Cybersicherheit nur eines von vielen komplexen, intersektoriellen Themen ist, denen sich der Staat heute zu widmen hat.

Im dritten Spannungsfeld zwischen Bürger und Wirtschaft gilt es, die Rahmenbedingungen für die Entwicklung eines erfolgreichen Sicherheitsökosystems zu setzen – der bisher am wenigsten beachtete Teil. Wie kann der Markt, der zudem mit dem Problem von Quasimonopolen der grossen Technologiekonzerne konfrontiert ist, so reguliert werden, dass eine optimale Balance zwischen Sicherheit und Funktionalität entsteht? Wie können Anreize zu mehr Sicherheitsverpflichtung für Anbieter von Dienstleistungen geschaffen werden?



In Demokratien müssen diese Konflikte auf politischer Stufe ausgetragen und systematisch angegangen werden. Ein Beispiel: Einerseits hat der Staat im Sinne einer konsequenten Strafverfolgung und modernen nachrichtendienstlichen Fähigkeiten Interesse an der Nutzung von Schwachstellen zur Überwachung. Andererseits hat er gleichzeitig auch ein Interesse an der grösstmöglichen Nutzung von sichereren Technologien durch Wirtschaft und Gesellschaft. Was die Debatte daher braucht, ist ein besseres Verständnis für unterschiedliche, gleichbedeutende Rollen, die der Staat im Bereich der Cybersicherheit wahrnehmen muss.

Neben der Rolle als Ordnungs- und Sicherheitshüter und als Gesetzgeber und Regulierer, tritt der Staat auch als Unterstützer der Gesamtgesellschaft, als Partner für die Privatwirtschaft, als Wissensschaffer und Wissensverbreiter und nicht zuletzt als Gefahr auf. Cybersicherheit muss in ihren multiplen Facetten verstanden werden, damit wir alle die politischen und gesellschaftlichen Probleme, die um das Thema herum entstehen, verstehen, einordnen und angehen können. Die Schaffung des nationalen Zentrums für Cybersicherheit bietet dafür eine gute Plattform.

Originalartikel auf Deutsch: Hier.

Originalartikel auf Englisch: Hier.

Bild: rawpixel.com