Grossbritannien: Die Cyber-Abwehr und die Rolle der Streitkräfte

Gemäss den strategischen Grundlagenpapieren Grossbritanniens stellt Cyber (tier one) eine von sechs Hauptbedrohungen für das Vereinigte Königreich dar (nebst kriegerischen Ereignissen, Terroranschlägen, Pandemien, etc.).

Martin Lerch

Mit der 2019 lancierten, gesamtstaatlichen und ministeriumsübergreifenden «Fusion Doctrine» und dem per 1. Januar 2020 neu gebildeten «Strategic Command» bei den Streitkräften fährt das UK einen sehr breiten und integrativen Ansatz im Bereich der Cyber-Abwehr.

Die Streitkräfte sind in die UK Cyber-Gesamtstrategie (defend, deter, develop) sehr eng eingebunden und unterstützen diese massgeblich. Das britische Verteidigungsministerium (UK MoD) ist sich der Bedeutung von Cyber-Risiken in den Streitkräften sehr bewusst und misst dieser Domäne (defensiv und offensiv) einen entsprechend hohen Stellenwert bei. Die Cyber-Abwehr stellt für die britischen Streitkräfte die «erste Linie der Verteidigung» dar.

Dabei zeichnen das MoD und die Streitkräfte primär für den Schutz der eigenen Netzwerke inklusive aller weltweit in Einsätzen stehenden Truppen und erst subsidiär für den generellen Schutz der UK Netzwerke (mit zivilen Partnerorganisationen) verantwortlich.

«Fusion Doctrine» und «Nationale Strategie zur Cyber-Sicherheit 2016 bis 2021»

Bei der «Fusion Doctrine» geht es darum, alle Kräfte (Privatsektor, Ministerien, Bevölkerung) einzubeziehen und zu integrieren im Bestreben, die Sicherheitsrisiken des Landes zu minimieren und das Vereinigte Königreich möglichst widerstandsfähig (resilient) zu machen. Dabei soll insbesondere die Cyber-Sicherheit optimal garantiert werden.

National Cyber Security Strategy 2016 bis 2021 (NCSS)[1]

Das noch gültige, 81-seitige Dokument, das die nationale Gesamtstrategie im Bereich Cyber festlegt, befindet sich in Überarbeitung. Es ist davon auszugehen, dass die Publikation der 3. Strategie aufgrund von Covid-19 und Brexit kaum zeitgerecht, aber immerhin 2021 erfolgen wird.

Die aktuelle Strategie beleuchtet auch das strategische Umfeld und die Verletzlichkeiten. Gemäss dem Dokument soll das UK bis ins Jahr 2021 im Hinblick auf mögliche Cyber-Bedrohungen sicher und resilient sein, was wirtschaftliche Prosperität und ein selbstbewusstes Verhalten in der Cyber-Domäne ermöglichen soll. Die strategische Ausrichtung stützt sich auf drei Pfeiler ab.

«**Defend**»: Es sollen die Mittel, Werkzeuge und das Personal bereitgestellt werden, um das UK vor Cyber-Gefahren zu schützen, auf Angriffe zu reagieren und sicherzustellen, dass Netzwerke, Daten und Systeme geschützt und resilient sind.

«**Deter**»: Es sollen feindliche Cyber-Aktionen erkannt, verstanden, untersucht und verhindert sowie Angreifer verfolgt und zur Rechenschaft gezogen werden.

«**Develop**»: Das UK fördert seine führende und innovative (world-class) Industrie im Bereich Cyber-Sicherheit, was entsprechende Forschung und Entwicklung bedingt. Die Strategie sieht über fünf Jahre ministeriumsübergreifende Investitionen im Bereich Cyber von £ 1,9 Mia. vor.

Institutionen und ihre Aufgaben

Strategische Ebene

Zuständig für das «Policy-Making», das heisst die gesamtstrategische Ausrichtung im Bereich Cyber-Abwehr, ist das «Cabinet Office», welches direkt der Regierung untersteht. Quasi der unterstützende «Arbeitsmuskel» für das Cabinet Office ist das «Cyber and Government Security Directorate» (CGSD), welches auch für das nationale Cyber-Security-Programm verantwortlich zeichnet.

Operationelle Ebene, GCHQ

Für den operationellen Schutz des Landes gegen Cyber-Risiken und für die Zusammenarbeit mit verschiedenen Regierungs- und Nichtregierungsbehörden ist schwergewichtig das «Government Communications Headquarters» (GCHQ) in Cheltenham verantwortlich. Das GCHQ (Deutsch: Regierungskommunikationszentrale und Signalaufklärungsdienst) ist der britische Nachrichtendienst, welcher sich ursprünglich mit Kryptografie, sicherer Datenübertragung und Fernaufklärung befasste; er ist dem Aussenministerium unterstellt. Die Hauptaufgaben sind heute sehr breit und umfassen (nebst den angestammten Segmenten) Bereiche wie Cyber-Sicherheit, Terrorabwehr, Organisierte Kriminalität, Unterstützung der Streitkräfte und generell die Erzielung eines strategischen Vorteils für das Vereinigte Königreich.

Leistungsbezüger sind das Verteidigungsministerium, der Inlandgeheimdienst (MI5), der Auslandsgeheimdienst (MI6), die «Serious and Organized Crime Agency» und diverse andere staatliche Stellen. Das Budget und die Angestelltenzahl werden nicht offiziell kommuniziert. Es wird davon ausgegangen, dass das GCHQ mindestens 6000 Personen beschäftigt.

Operationelle Ebene NCSC

Im Bereich der Cyber-Verteidigung des UK ist das «National Cyber Security Centre» (NCSC) federführend. Nach informellen Informationen arbeiten bei dem im Oktober 2016 gegründeten NCSC ca. 1000 Mitarbeitende, davon rund 300 in London Victoria, die restlichen ca. 700 beim GCHQ in Cheltenham.

Das NCSC ist die operationelle Führungsspitze der UK Cyber-Sicherheit und als solches Teil des GCHQ. Das NCSC ist vor allem auch Anlaufstelle für kleine und mittlere Unternehmen, grössere Organisationen und Regierungsorganisationen. Es arbeitet mit anderen UK-Organen wie den Strafverfolgungsbehörden,

den Streitkräften, den Nachrichtendiensten, den Betreibern von Kritischer Nationaler Infrastruktur (KNI), sowie mit der Industrie und internationalen Partnern sehr eng zusammen. Seine Bedeutung ist gerade auch wegen Covid-19 und den zunehmenden Cyber-Attacken nochmals gestiegen.

Rolle und Aufgaben des Verteidigungsministeriums und der Streitkräfte

Das Verteidigungsministerium ist primär für den Schutz der eigenen Netzwerke und für die Kommunikation mit «Overseas-Truppen», sowie subsidiär für die Verteidigung der UK-Netzwerke verantwortlich.

Die Aufgaben der Streitkräfte im Cyber-Bereich sind ebenfalls der Eigenschutz bzw. die Sicherstellung der Cyber-Verteidigung der eigenen Netzwerke und die Unterstützung der zivilen Behörden bei grossangelegten, nationalen Cyber-Attacken. Es soll, vor allem durch die vorhandenen Offensivmittel, eine abschreckende Wirkung gegen aussen erzielt werden. Grundsätzlich sollen die Streitkräfte die Fähigkeit haben, auf Cyber-Attacken genauso angemessen reagieren zu können, wie auf andere Angriffe.

Bei der Erfüllung dieser komplexen Aufgaben spielt das neu gebildete Strategic Command (SC) eine zentrale Rolle. Dieses zeichnet insbesondere verantwortlich, die Cyber-Fähigkeiten der Teilstreitkräfte mit dem Ziel zu koordinieren, militärische Operationen durchzuführen. Im Dezember 2019 hat das MoD die Umbenennung des früheren «Joint Forces Commands» (JFC) in «Strategic Command» (SC) umgesetzt und diesem im Cyber-Bereich die folgenden zusätzlichen Aufgaben übertragen: Verantwortlichkeit für die domänenübergreifenden Cyber-Fähigkeiten im Bereich der strategischen Konkurrenz und Konfrontation («strategic competition and confrontation»); Sicherstellung der internationalen Interoperabilität, insbesondere im Rahmen der NATO und der «Joint Expeditionary Force»; Weiterentwicklung der Informationsbeschaffung und den Lead bei der Führung in der Cyber-Domäne für die Streitkräfte.

Das SC kann sich für seine komplexen Aufgaben auf die «Joint Forces Cyber Group» (JFCG) abstützen. Diese koordiniert die Ressourcen und Kapazitäten der Cyber-Einheiten der klassischen Teilstreitkräfte (Army, Navy, Air Force) und hat zudem die Aufgabe, die «Joint Cyber Units», «Joint Information Assurance Units» und die «Cyber Reserves» zu führen. Integriert ist das «Computer Emergency Response Team» des MoD, welches für die notfallmässige Antwort auf Cyber-Vorfälle verantwortlich zeichnet.

Trends beim Ministerium und bei den Streitkräften

- Seit 2018 hat das MoD pro Jahr über £ 40 Mio. in die Entwicklung neuer «Cyber Security Operations Capabilities (CSOC)» investiert. Diese verbessern die Fähigkeiten des UK, Systeme und Netzwerke vor Cyber-Angriffen zu schützen und konsolidieren die Zusammenführung der defensiven Cyber-Aktivitäten;

Zehn Schritte zur Cyber-Sicherheit, Empfehlungen des NCSC für die Öffentlichkeit.

Grafik: National Cyber Security Centre

- Im März 2018 wurde die «Defence Cyber School» an der «Defence Academy» in Shrivenham eröffnet. Zusammen mit dem «Global Operations and Security Control Centre» und dem «Computer Emergency Response Team» werden «Rapid Response Teams» ausgebildet, welche im UK und im Ausland schnell und effektiv auf feindselige Cyber-Aktivitäten reagieren können;
- Seit 2018 besteht das «Cadets CyberFirst Programme», welches gemeinsam vom Verteidigungsministerium und vom NCSC ins Leben gerufen wurde. Jährlich werden über 2000 Kadetten darin unterrichtet, mit dem Internet verbundene Systeme vor Cyber-Attacken zu schützen;
- Seit 2019 werden zusätzliche, signifikante Investitionen getätigt, um die offensiven Cyber-Fähigkeiten zu verbessern, eine ministeriumsübergreifende «command and control» Struktur einzurichten und die Resilienz der UK-Netzwerke gegenüber Online-Attacken zu verbessern («National Cyber Force»); dies als Pendant zum NCSC;[2]
- Seit Mai 2019 befinden sich mehrere «Army cyber operations centres» im Aufbau. Diese sollen nachrichtendienstliche Informationen sowie freie Quellen nutzen, um die «British Army» rund um die Uhr mit Informationen und Analysen zu versorgen, Falschinformationen zu erkennen, um den Streitkräften sowie ihren Verbündeten einen Informationsvorsprung bezüglich Cyber-Gefahren zu verschaffen.

Britisch-schweizerische Cyber-Austauschplattform

Das Thema Cyber hat – wie überall – auch im UK einen sehr hohen Stellenwert. Deshalb hat der schweizerische Verteidigungsattaché auf der Schweizer Botschaft in London 2019 bereits zum dritten Mal erfolgreich ein Cyber-Defence-Symposium durchgeführt.

Es handelt sich dabei um eine seit 2017 etablierte Plattform, die den Austausch im Cyber-Bereich zwischen Grossbritannien und der Schweiz fördert. Sie dient dem Austausch im Cyber-Bereich nicht nur in den Segmenten Sicherheits- und Verteidigungspolitik, sondern auch auf den Ebenen Industrie, Wissenschaft und Hochschulen. Entsprechend sind auch Organisationen wie der Swiss Business Hub, Präsenz Schweiz und die gesamte Botschaft ins Projekt involviert. Das Symposium

Begrüssung zum Security and Defence Symposium 2019 auf der Schweizer Botschaft in London durch Verteidigungsattaché Oberst i Gst M. Lerch, die Chefin des Swiss Business Hub, M. Hood, und Botschafter A. Fasel. (v.l.n.r). Bild: Autor

gliedert sich strukturell in die drei Bereiche: Keynote Referate, Panel-Diskussion und zur Abrundung durch einen Netzwerkanlass «Swiss style».

Die bisherigen Symposien haben sich mit folgenden Themen befasst:

2017 ging es um die Cyber-Abwehr im militärischen und industriellen Sektor. Als militärische Vertreter sind der damalige Delegierte für Cyber im VBS und der Cyber Commander der UK Streitkräfte aufgetreten.

Im folgenden Jahr ging es um Fragen der Resilienz und um den Schutz der kritischen Nationalen Infrastruktur. Aufgetreten sind unter anderen ein Vertreter des BABS und der BKW und aus dem UK Vertreter des Cabinet Office und des NCSC. Das Symposium 2019 war dem Thema «Autonomous Systems, Drones and Artificial Intelligence (AI), from a military and industrial perspective. UK and Swiss approach» gewidmet. Nebst anderen sind dabei Vertreter der British Army und von armasuisse aufgetreten. Ein hochrangiger Vertreter des britischen Oberhauses hat den Anlass jeweils moderiert.

Das Symposium hat sich in London innert drei Jahren zu einer fest etablierten Plattform entwickelt zwischen Vertretern von VBS/Schweizer Armee, den britischen Streitkräften und Cyber-Abwehrorganisationen, den Industrien beider Länder sowie von Vertretern von Hochschulen. Er ermöglicht einen interessanten Wissens- und Erfahrungsaustauch vor allem in den Bereichen Cyber Defence, technologische Entwicklungen und Innovationen. Der Anlass 2020 war im Detail vorbereitet, konnte jedoch wegen Corona nicht durchgeführt werden.

Der Anlass hat sich so gut etabliert, dass das Verteidigungsministerium diesen fix in sein Jahresprogramm für die Verteidigungsattachés aufgenommen hat (als einzigem von einer Botschaft durchgeführtem Anlass).

Die dynamisch-innovativ-adaptiven Entwicklungen im Cyber-Bereich im UK, bzw. in den UK-Streitkräften sind für die Schweiz und die Schweizer Armee im Sinne eines Benchmarks von hohem Interesse und können bei einem entsprechenden Austausch von ebensolchem Nutzen sein.

Als baldige EU-Drittstaaten (UK nach dem 31.12.2020) ergeben sich für die Schweiz und für Grossbritannien in Zukunft vielversprechende Austausch- und Kooperationsfenster («windows of opportunities»), die genutzt werden sollten. ■

1 HM Government – National Cyber Security Strategy 2016–2021 (pdf, 81 Seiten): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

2 GOV.UK. 2019. Cyber innovation at the forefront of UK's approach to modern warfare. https://www.gov.uk/government/news/cyber-innovation-at-the-forefront-of-uks-approach-to-modern-warfare.

Oberst i Gst
Martin Lerch
MAS spcm ETHZ
RA, Verteidigungsattaché
London von 2015–2020
4900 Langenthal