# Cyberspionage und Datensicherheit: Der Westen im Fadenkreuz?

## Fazitbericht | 15. FFS Security Talk vom 22. November 2023, Hotel Schweizerhof, Bern

Mit dem Siegeszug des Internets und der damit verbundenen fortschreitenden Digitalisierung entstand während der letzten zwei Jahrzehnte ein hochkomplexer Cyberraum, durch welchen die Vernetzung der ganzen Welt erreicht wurde. Dieser digitale Raum eröffnet einerseits eine Vielzahl an neuen Möglichkeiten, gleichzeitig ist er aber auch brandgefährlich. Hackerangriffe auf staatliche Institutionen und Unternehmen im Westen haben in den letzten Jahren massiv zugenommen. Auch in der Schweiz war dieser Trend klar nachverfolgbar, wie eine Vielzahl von Beispielen in vergangenen Jahr aufzeigt. Auch Privatwirtschaftliche Akteure bleiben nicht verschont und werden immer häufiger Ziel solcher Attacken.

Welche Sektoren und Institutionen stehen im Fokus solcher Angriffe? Wie können und müssen Behörden, Institutionen und Unternehmen ihre kritischen Daten vor Cyberangriffen schützen? Wie muss die Politik mit der Bedrohung durch Cyberspionage und andere Cybergefahren umgehen? Welche Massnahmen sind dringlich und nötig?

Diese und weitere wichtige Fragen diskutierten beim 15. FSS Security Talk in Bern namhafte Expertinnen und Experten wie **Generalmajor Jürgen Setzer** (Stellvertreter Inspekteur CIR und CISO, Bundeswehr), **Dr. Myriam Dunn Cavelty** (Leitende Dozentin für Sicherheitsstudien, Center for Security Studies (CCS), ETH Zürich), **Nicolas Mayencourt** (Founder & Global CEO, Dreamlab Technologies), **Franz Grüter** (Verwaltungsratspräsident green.ch-Gruppe; Nationalrat SVP, LU) sowie **Johann Alessandroni** (Leiter der Abteilung Information Security Governance, Excellium Services by Thales Group).

**Hans-Jürg Käser**, Präsident des FORUM SICHERHEIT SCHWEIZ, begrüsste die fast 120 Teilnehmenden mit ein paar einleitenden Worten am 15. FSS Security Talk. Um dem straffen Programm Rechnung zu tragen begann jedoch sogleich Herr Generalmajor Setzer mit dem ersten Input-Referat.

## Referat Generalmajor Jürgen Setzer

Generalmajor Setzer werde oft gefragt, wie man in seiner Funktion als Stellvertreter Inspekteur Cyber- und Informationsraum und Chief Information Security Officer der Bundeswehr überhaupt noch schlafen könne in der Nacht. Seine Antwort sei einfach: «Indem man am Tag hellwach ist». Der Schutz des Cyber- und Informationsraum werde in der Bundeswehr grossgeschrieben. Deshalb wurde der **Cyber- und Informationsraum (CIR)** der Bundeswehr im April 2017 auch als **eigenständiger militärischer Organisationsbereich** aufgestellt und somit auf eine Ebene gehoben mit den **übrigen Dimensionen Land, Luft, Wasser und Weltraum**.

### Cyber- und Informationsraum als militärisches Einsatzgebiet

Die Bedeutung des Cyber- und Informationsraumes als militärisches Einsatzgebiet zeige sich beispielsweise sehr deutlich im aktuellen russischen Angriffskrieg gegen die Ukraine. Obwohl die Berichterstattung größtenteils auf den konventionellen kinetischen Fähigkeiten der Streitkräfte liege, könne dennoch täglich festgestellt werden, dass die **Fähigkeiten im Cyber- und Informationsraum ein wesentlicher Bestandteil der Kriegsführung** seien. Insbesondere die Medien fungierten dabei als Schauplatz und Akteur der russischen Informationskriegsführung, mit dem übergeordneten Ziel, den Verteidigungswillen der Ukraine und ihrer Verbündeten zu brechen. Deutschland, obwohl keine Kriegspartei, sei permanent hybrider Einflussnahme ausgesetzt, sei es durch Informationskampagnen oder Cyberattacken, mit dem Versuch, die politische Willensbildung zu beeinflussen. Die Akteure umfassten dabei sowohl reguläre Cyberkrieger russischer Geheimdienste als auch kriminelle Organisationen und Gruppierungen. Es werde deutlich, dass **staatliche Akteure nichtstaatliche Akteure gerne nutzten, um Angriffe durchzuführen und die Verantwortung von sich zu weisen**, was die eindeutige Attribution der Vorfälle erschwere, sowohl für Deutschland als auch für andere Länder und Bündnispartner. Der Angriff Russlands auf die Ukraine und die begleitenden Cyberangriffe bergen auch indirekt eine erhebliche Gefahr für Deutschland. Ein Beispiel dafür sei die Cyberattacke Russlands gegen den vom ukrainischen Militär genutzten Satellitendienst KA-SAT von Viasat, bei der auch die Betreiber von Windkrafträdern in Deutschland betroffen waren, da die Fernwartung der Windanlagen ebenfalls über KA-SAT lief.

Eine ähnlich große Bedeutung des Cyber- und Informationsraums in militärischen Konflikten lasse sich derzeit auch im Zusammenhang mit dem Krieg zwischen Israel und der Hamas beobachten. Der Angriff der Hamas-Terroristen werde parallel durch Operationen im Cyberraum begleitet. Opfer seien dabei bereits wichtige Informationsmedien wie die Nachrichtenagentur Jerusalem Post oder auch ein israelisches Gefahrenabwehr-Informations- und Warnsystem geworden, welches angesichts der ständigen Raketenangriffe ein essenzielles, lebensrettendes Instrument für die israelische Bevölkerung darstellt.

### Informationen als Schlüsselressource modernen Gesellschaften und Streitkräfte

Solche Angriffe würden natürlich einerseits Angst und Verwirrung in der Bevölkerung schüren. Andererseits sei das Ziel dieser Angriffe oft auch, gegnerische Informationen zu beeinträchtigen, da diese eine Schlüsselressource moderner Gesellschaften darstellten und eine Voraussetzung für die Einsatzbereitschaft der Streitkräfte seien. Der Informationssicherheit, also dem erfolgreichen Schutz der Informationsübertragung, Informationsverarbeitung und Informationsspeicherung, komme daher eine besondere Bedeutung zu. **«Die Informationsüberlegenheit ist schliesslich Voraussetzung für Entscheidungsüberlegenheit, Voraussetzung für Wirkungsüberlegenheit und am Ende des Tages Voraussetzung für die Siegesfähigkeit von Streitkräften in einem Konflikt»**, unterstrich der Generalmajor die Schlüsselrolle der Information.

Auch die Bundeswehr werde tagtäglich Ziel von Angriffsversuchen im Cyber-Space. Als Chief Information Security Officer freue er sich zwar zu sagen, dass bisher keiner dieser Angriffe erfolgreich gewesen sei. Jedoch müsse man mit diesen Aussagen immer vorsichtig sein, denn man könne nie zu 100 % ausschließen, dass jemand bereits ins eigene System eingedrungen sei und von den Schutzmechanismen noch nicht bemerkt wurde.

Diese Angriffe führten demnach vor Augen, dass es zu jedem Zeitpunkt wichtig sei, hellwach, innovativ und agil zu sein und die eigene Sicherheitsarchitektur ständig zu überprüfen und zu verbessern. Hierfür habe man vier Handlungsfelder definiert: den Faktor Mensch, die Konzepte und Technik, den Ausbau des Innovationsumfeldes sowie die nationale und internationale Kooperation.

**Der Faktor Mensch**

Das erste Handlungsfeld, der Faktor Mensch, verkörpere dabei einen ganz entscheidenden Faktor auch in der IT-Sicherheit. Zum einen aus dem Blickwinkel der Nutzer beziehungsweise der Nutzerinnen: **Über 80 % der erfolgreichen Angriffe auf die IT-Sicherheit könne man auf das ungewollte Mitwirken des Nutzers oder der Nutzerin zurückführen.** Die Methoden der Täter seien dabei vielfältig. Der Begriff Social Engineering umfasse zahlreiche Strategien, die darauf abzielen, Menschen zu beeinflussen, zu manipulieren und bestimmte Verhaltensweisen hervorzurufen, wie beispielsweise die Zugriffsgewährung auf Daten und Systeme sowie das Teilen von Informationen. Mit den Fortschritten im Bereich der KI hätten sich auch die Möglichkeiten verbessert, Opfer erfolgreich zu täuschen. Ein jeder unter den Anwesenden habe sicherlich schon Phishing-E-Mails erhalten, sei es auf privaten, aber auch auf den Dienst- beziehungsweise Geschäfts-E-Mail-Adressen, die teilweise täuschend echt wirkten. Positiv sei jedoch festzustellen, dass durch die Angriffe im Kontext mit dem russischen Angriffskrieg auf die Ukraine die Awareness bei den Nutzerinnen und Nutzern grundsätzlich zugenommen habe. Ausreichen würde dies jedoch noch nicht. Deshalb stelle man sich in der Bundeswehr entsprechend der realen Gefahrenlage auch 7 Tage die Woche, 24 Stunden am Tag mit Selbst-Challenges, um mögliche Schwächen zu erkennen, bevor diese von anderen ausgenutzt werden

können. Dabei greife man sich mit den offensiven Kräften selbst an, sensibilisiere die Mitarbeiter und Mitarbeiterinnen und verstärke das Bewusstsein, dass man tagtäglich unter Beschuss steht.

Daneben stellten jedoch auch der **deutlich gestiegene Bedarf an Cyber-Sicherheitsfachpersonal und ihm gegenüberstehend ein wachsender Fachkräftemangel Herausforderungen dar** und machten es notwendig, auch neue Wege zu beschreiten, um genügend geeignetes Personal zu finden. Ein besonderer Fokus liege daher auf der Ausbildung. Die Bundeswehr bilde daher auch eigenständig aus, mitunter an ihrer eigenen IT-Schule oder auch an den Universitäten in Hamburg und München.

**Konzepte, Technik, Innovation und Kooperation**

Das zweite Handlungsfeld betreffe die verwendeten Konzepte und Techniken. Die Bundeswehr verfüge standardmäßig über Informationssicherheitskonzepte. Diese seien die Grundlage für alle Verbände, bevor sie in den Einsatz gingen, seien dies Einsätze im normalen Krisenmanagement, wie derzeit noch in Mali oder im Kosovo, oder auch einsatzgleiche Verpflichtungen im Kontext der Abschreckung oder an der Ostflanke der NATO, beispielsweise in Litauen.

Zugleich beschäftige man sich auch mit neuen und zukünftigen Konzepten und Techniken, respektive dem Ausbau des Innovationsumfeldes, das 3. Handlungsfeld. **Cybersicherheit sei kein statischer Zustand.** Sie erfordere kontinuierliche **Anpassung** und **Weiterentwicklung**, um mit den **kurzen Innovationszyklen**, die in der Digitalisierung erlebt werden, auch in der Cyber-Sicherheit Schritt zu halten. Drei Aspekte seien in diesem Zusammenhang unter dem Gesichtspunkt des Innovationsumfeld für von besonderer Relevanz: Effektivität, Bedarfsorientierung und Agilität.

Zur Erhöhung der Effektivität sei ein etablierter IT-Dialog und Innovationsdialog mit Partnern aus der Wirtschaft wie beispielsweise dem Bitkom, dem Branchenverband der deutschen Informations- und Telekommunikationsbranche, genauso wichtig wie mit bundes- und länderinternen Sicherheitsbehörden oder auch der Wissenschaft und Forschungseinrichtungen. Daneben müsse zur Erhöhung der Bedarfsorientierung natürlich auch ein Dialog innerhalb der Streitkräfte vorhanden sein. Der Innovationsdialog setzt bei der Bundeswehr auf einen implementierten Wirkverbund zwischen den Verantwortlichen für die Digitalisierungsplattform, dem Beschaffungsamt und den privatwirtschaftlichen IT-System-Dienstleistern. Dieser Wirkverbund verkörpere das Schlüsselelement für die **schnelle** und **nachhaltige digitale Transformation** und funktioniere nur, wenn **Anwender**, **Entwickler** und **Beschaffer Hand in Hand von Anfang an im gleichen Boot sitzen** und zusammenarbeiten.

Darüber hinaus verfüge die Bundeswehr auch über anwendungsleitende Innovationsakteure. Dazu zähle zum einen der Cyber Innovation Hub als zentraler Fokuspunkt für die Erprobung von marktverfügbaren Lösungen aus der Welt der Startups. Daneben gebe es die sogenannte "BWI Schmiede", die als Coding Force entscheidend zur Digitalisierung und Automatisierung der Bundeswehr beitrage. Ressortübergreifend sei zudem zur Förderung von Forschungsprojekten im Kontext der Cyber Sicherheit eine Cyber Agentur aufgebaut worden. **«Im Cyberbereich existiert keine Grenze zwischen innerer und äußerer Sicherheit, und deshalb müssen die Kräfte für die innere und äußere Sicherheit gemeinsam ihre Fähigkeiten nach vorne treiben»**, betonte Generalmajor Setzer erneut die Notwendigkeit einer ressort- und ebenenübergreifenden Zusammenarbeit. Zu diesem Zweck und um den Ansatz der stetigen Verbesserung und der Innovation genügend Gestaltungsspielraum über innere und äußere Grenzen hinweg zu bieten, sei diese Cyberagentur geschaffen worden. Weiter unterhalte man z.B. auch Kooperationen mit der Fraunhofer-Gesellschaft und den beiden Bundeswehruniversitäten.

**«Nicht ein Spieler auf dem Platz bestimmt das Geschehen, sondern viele Spiele zusammen»**

Beim vierten Handlungsfeld gehe es um nationale und internationale Kooperation und Übungen. Die ressortübergreifende Zusammenarbeit auf nationaler Ebene zwischen Forschung, Sicherheitsbehörden und Unternehmen werde als von entscheidender Bedeutung angesehen. Die deutsche Cybersicherheitsstrategie mache dazu auch klare Vorgaben. Der Kristallisationspunkt in Deutschland sei dabei das Nationale Cyber-Abwehrzentrum. Bereits 2011 sei es implementiert worden unter der Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Es sei das erste Forum der staatlichen Zusammenarbeit im Kontext der Cyber-Sicherheit gewesen. In den Folgejahren lag der Fokus darauf, dieses Forum sukzessive weiterzuentwickeln und die Anzahl der Teilnehmenden fortlaufend zu steigern. Dies sei wichtig, denn bei der Cyberabwehr handle es sich um ein Mannschaftsspiel: «Nicht ein Spieler auf dem Platz bestimmt das Geschehen, sondern viele Spieler zusammen». Aber eins sei auch klar, ohne einen überzeugenden Kapitän beziehungsweise Trainer funktioniere es nicht. Deswegen habe man sich dazu entschlossen, Koordinatoren zu definieren. Die Bundeswehr nehme dabei immer die Rolle als stellvertretender Koordinator ein, um den Übergang von Frieden zu Krieg auch im Koordinationsgremium stets sicherstellen zu können.

Diese als Informationskoordinations- und Kooperationsplattform ausgeworfene Instanz des Nationalen Cyber-Abwehrzentrums leiste somit einen wesentlichen Beitrag zur Cyber-Sicherheit, bereits heute und jetzt. **Der Staat habe die Verantwortung, für einen digitalen Super-GAU vorbereitet zu sein, und zwar bevor dieser tatsächlich eintrete.** Unerlässlich hierfür sei das gemeinsame Üben unserer Sicherheitsbehörden, der Bundeswehr, der Kommunen, der Behörden und KRITIS-Unternehmen, wie es im September dieses Jahres bei der länder- und ressortübergreifenden Krisenmanagementübung LÜKEX geschehen sei. Während der dabei simulierten bundesweiten Cyberangriffe sei das vorrangige Ziel gewesen, die Staats- und Regierungsfunktion aufrechtzuerhalten. Denn wenn diese nicht mehr gewährleistet seien, dann sei Chaos Vorschub geleistet. Nur durch solche gemeinsamen Übungen könne man entscheidende Impulse zur Verbesserung der Resilienz schaffen für Szenarien, die zwar noch nicht eingetreten sind, aber die eintreten könnten.

**Internationale Kooperation**

Von Bedeutung sei auch der Austausch auf multilateraler Ebene. Man freue sich in diesem Zusammenhang besonders über die engen Bindungen zu den Schweizer Partnern, sei es beispielsweise durch die jährlichen Treffen der Cyber-Commander des DACH-Raumes oder gemeinsame deutsch-schweizerische Seminare zu Führungs-Information-Systemen und Datenstrategien. Weiter blicke der Cyber- und Informationsraum auch schon freudig auf den Besuch des Schweizer Cyber-Commanders und des Stabchefs Operative Schulung in Bonn im nächsten Jahr.

Neben diesem Austausch sei auch das kontinuierliche Üben eine der Voraussetzungen für eine schlagkräftige Cyberabwehr. **Auch dort habe man im Rahmen von "COMMON ROOF" eine gute und tragfähige Verbindung zu den Schweizer Freunden.** Dabei handle es sich um eine jährlich wiederkehrende Übung mit dem Ziel, die Fähigkeitsentwicklung der DACH-Nationen in der Operabilität zu üben. Auch mit Blick in die Zukunft pflege man im DACH-Format eine gewinnbringende Zusammenarbeit. Im Rahmen der multilateralen Cyber-Defence-Exercise im nächsten Jahr werde man gemeinsam im Dachformat und ursprünglich vorgesehen auch mit den israelischen Freunden, die Cyber- und Emergency-Response-Teams gemeinsam beüben.

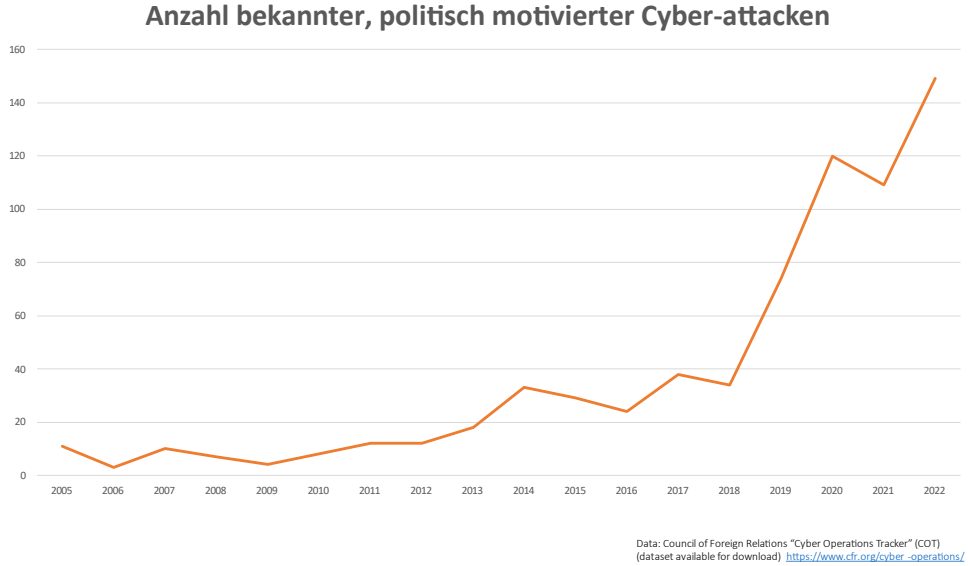
«**Information ist die Schlüssel-Ressource unserer modernen Gesellschaft und unserer Streitkräfte.** Ihr Schutz, das heißt die Cyber-Informations-Sicherheit ist für uns alle, Deutsche sowie Schweizerinnen und Schweizer, eine Pflicht und zugleich eine der größten Herausforderungen. Betrachten wir diese Herausforderung als Chance. Eine Chance, unsere Fähigkeiten gemeinsam zu entwickeln unsere Länder zu schützen und unsere Zukunft gemeinsam zu gestalten.»

## Referat Dr. Myriam Dunn Cavelty

Als zweite Rednerin legte Myriam Dunn Cavelty den Fokus auf die Cyberspionage, welche sie aus einer wissenschaftlichen Perspektive beleuchtete. Ihr Ziel war es aufzuzeigen, warum wir vor allem von Spionage sprechen, wenn es um staatliche Aktivitäten im Cyberraum geht und weniger von anderen gängigen Formen von Cyberangriffen, für die es keine so grossen Kapazitäten bräuchte.

### Anstieg politisch motivierter Cyber-Attacken seit 2017 /2018 - Cyberspionage an Spitze

Wenn man die Datenlage beobachte, sehe man einen massiven Anstieg der Anzahl öffentlich bekannter, politisch motivierter Cyber-Attacken um die Jahre 2017/2018 herum. Zurückzuführen sei dieser Anstieg einerseits auf den Auf- und Ausbau von Kapazitäten im Cyberraum nach 2010. Heutzutage existierten mehr Akteure, welche solche gezielten Attacken überhaupt durchführen könnten. Weiter hänge der Anstieg aber auch mit einem Ausbau der Kapazitäten auf Seiten der Verteidigung und der Fähigkeiten zur Detektion solcher Attacken zusammen. Wie schon von Generalmajor Setzer gehört wurde und werde viel in die Cybersicherheit investiert.




Wenn man nun die Art der Attacken anschaue, sehe man, dass die Spionage mit großer Mehrheit oben aufschwimme. Von den bekannten politisch motivierten Attacken seien 70-80 % Spionage. Und hierbei handle es sich nur um die bekannten Daten. Wenn man berücksichtige, dass die Spionage möglichst im Verborgenen betrieben wird, dann sei davon auszugehen, dass die effektive Zahl noch grösser ist.

### Kapazitäten / Konfigurationen / Kontext – Gute Gründe für Cyberspionage

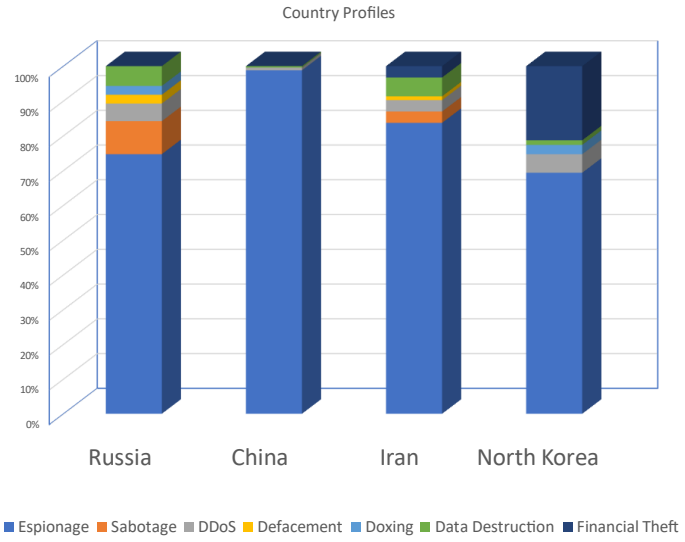
Drei Gründe seien dafür verantwortlich, dass die Spionage als staatliches Mittel im Cyberraum so weit verbreitet ist: Zum einen die eben schon erwähnten Kapazitäten bzw. in diesem Zusammenhang die sogenannten **«Advanced Persistent Threats»**, kurz **APTs**. Als zweites die **Konfigurationen**, welche die technischen Eigenschaften von Systemen und die Möglichkeit darauf einzuwirken umfassen, aber auch den Faktor Mensch und dessen Kompetenzen im Cyberbereich. Und schliesslich liefere auch der geopolitische Kontext respektive das Konzept der **«strategic competition»** eine Erklärung dafür, wieso die Cyberspionage für Staaten viel Sinn ergibt.

**Kapazitäten**

Thematisiere man die Kapazitäten müsse man zuerst verstehen, dass es gewisse Aktivitäten im Cyberraum gebe, die sehr schwierig durchzuführen seien. «Die Vorstellung des Hackers, der im Keller sitzt und irgendwelche Knöpfe drückt, um etwas Großes hervorzubringen, muss man in diesen Fällen aus den Köpfen der Leute streichen.» Diese Einsicht sei nötig, um zu erkennen, wem man eigentlich gegenüberstehe und welche Maßnahmen ergriffen werden könnten.

Länderprofile

- Seit 2005: 34 Länder führen offensive Cyber-operationen durch
- China, Russland, Iran, Nord Korea verantwortlich für 77% aller Operationen
- Achtung, Visibilität!




Betrachte man die Länderprofile der Länder, welche seit 2005 Cyber-Operationen des höheren Segments durchgeführt haben, dann sehe man, dass dies 34 Länder seien. **Ungefähr 77 % davon** gingen auf die **vier Akteure Russland, Iran, China und Nordkorea** zurück, also politische Rivalen der USA. Wichtig sei jedoch, dass man auch hier wieder die Visibilität thematisiere. Die Daten, welche vorliegen, würden von Firmen, sogenannten Threat Intelligence Companies, bereitgestellt, welche ihren Sitz mehrheitlich in den USA haben. Diese hätten die Kapazitäten und Fähigkeiten zum Erfassen solcher Attacken jahrelang aufgebaut, während anderen Ländern diese Kapazitäten fehlten, was dazu führe, dass auch die wissenschaftliche Datengrundlage unvollständig sei.

Wie oben bereits erwähnt, mache die Spionage einen Großteil der staatlichen Cyber-Operationen des oberen Segments aus – insbesondere auch bei den Hauptrivalen der USA. Die Einheiten, welche diese Spionage-Aktivitäten ausführten, würden auch als Advanced Persistent Threats, kurz APTs, bezeichnet. Sie zeichneten sich durch hochentwickelte, über Jahre anhaltende, und von Menschen ausgehende Fähigkeiten aus. Neben einem **tiefgehenden technischen Know-how** seien solche **Cyberoperationen** auch **sehr kostspielig**. Dies führe dazu, dass **APTs meist staatlich gesteuert** seien und an **sensiblen, wertvollen Daten interessiert seien**, damit sich der Aufwand hinter solchen Operationen auch lohne.

**Konfigurationen**

Beschäftige man sich mit den Konfigurationen, welche Cyberoperationen begünstigen, dann stelle man fest, dass Angreifer Zeit benötigen, bis Verwundbarkeiten gefunden und die Programme fertiggestellt sind, um die gefundenen Verwundbarkeiten auch wirklich auszunutzen. Meist vergingen dabei Monate, wenn nicht sogar Jahre. Weiter würden sich Cyberoperationen lohnen, wenn man dabei im Verborgen agieren kann und will, was mit den Anforderungen der Spionage übereinstimme. Da der Zugang zu einem Netzwerk nicht mit Gewalt hergestellt werden könne, seien **existierende Verwundbarkeiten** und

die **Fähigkeit unentdeckt zu bleiben wichtig**. Wenn ein Angreifer im System auffliegt, könne es sein, dass er sein gesamtes, kostspieliges und mit großem Aufwand entwickeltes Toolset verliere. Cyberoperationen würden sich auch lohnen, wenn man keine hohe Intensität oder Zerstörung damit anpeile. Es sei nämlich nicht einfach, einen zerstörerischen Effekt genau zu timen und das Ausmaß des Effekts vorherzusehen. Das bedeute auch, dass es **militärisch gesehen wenig Sinn mache, mit Cyberoperationen Netzwerke zerstören zu wollen**; stattdessen mache dort **der physische Weg mehr Sinn**. Das heißt, je intensiver der angepeilte Effekt und je komplexer die Operation, desto eher fliege ein Angreifer auf und riskiere seine Investitionen. Und zuletzt würden sich Cyberoperationen lohnen, wenn ihr Effekt nicht vollständig kontrolliert werden muss. **Cyberoperationen** finden in **gegnerischen Systemen** statt, die oft **nicht vollständig bekannt** seien, und darum könnten die **Effekte einer Operation** meist auch nicht **vollständig getestet oder vorhergesagt werden**. Daraus entstünden dann auch oft die Kollateralschäden, die sich bei vielen Cyberangriffen beobachten ließen.

Wenn nun diese 4 Punkte zusammengebracht würden und man sich anschaue, welche Art der Cyberoperationen sich bei Netzwerken mit erhöhter Sicherheit lohnen, sei man wieder bei der Spionage.

**Kontext und Strategic Competition**

Schliesslich liefere auch der geopolitische Kontext eine Erklärung für die Verwendung von Cyberspionage als staatliches Mittel. Dabei schlage sie die **Strategic Competition** als Rahmen vor, der es erlaube zu verstehen, warum gewisse Aktivitäten im Cyberraum vermehrt beobachtet werden können. Bei der Strategic Competition handle es sich um ein aus den USA stammendes Konzept. In diesem Konzept sehe man eine aktive **Verwischung von Krieg und Frieden**, und hierfür eigneten sich Cyberoperationen auch wieder. Alle Cyberoperationen, beispielsweise auch in der Ukraine, würden mit Absicht unter der Kriegsschwelle gehalten, in einer hybriden Form zwischen Krieg und Frieden. Bei der Strategic Competition gehe es um das Nutzen aller Machtbereiche, und deshalb eigne sie sich auch als Großmachtspiel. Dabei würden sehr große Ressourcen mobilisiert, und wenn man nun wieder zur Cyberspionage komme, dem systematischen Stehlen von geistigem Eigentum, stelle diese auch hier

wieder ein sinnvolles Mittel für Staaten dar, um eine Machtressource anzuhäufen. Es sei zwar weiterhin sehr schwierig, die Effekte und Schäden von Spionage zu messen, auch aus wissenschaftlicher Sicht. Es herrsche jedoch unterdessen Klarheit, dass eine **kumulative Strategie**, also **wiederholte, kleinere, niederschwellige Attacken**, **gewinnbringender** sind als eine **große zerstörerische Attacke**. Man sehe also, dass all diese Faktoren die Verwendung von Spionage als staatliches Mittel im Cyberspace begünstigten.

Zum Schluss betonte Frau Dr. Dunn Cavelty jedoch, dass, auch wenn sie hier vor allem über Cyberspionage gesprochen habe, die Fähigkeiten zur Cyberspionage eng verknüpft seien mit den Fähigkeiten für andersartige Cyberoperationen. Man müsse sich also bewusst sein, dass mit dem **Ausbau der Fähigkeiten im Cyberspace**, der in den letzten Jahren zu beobachten war, auch die **Gefahr von Operationen steige**, welche das Potenzial hätten, die **gesellschaftlichen Ordnung massgeblich zu stören.**

## Referat Nicolas Mayencourt

Nicolas Mayencourt fokussierte sich in seinem Inputreferat auf Vulnerabilitäten, also auf Angriffsflächen und Schwächen im Cyberraum, mit dem Ziel, dass diese erkannt und entsprechend gehandelt werde. Obwohl die Schweiz eine so kleine Nation sei, sei ihre Innovationskraft eindrücklich und deshalb sei es ihm auch ein spezielles Anliegen, dass die Gefahren und Methoden diese Innovationskraft zu schützen bekannt seien.

### Von der natürlichen zur Welt 2.0

Wenn wir uns mit den Vulnerabilitäten im Cyberspace befassten, sei es sinnvoll, zuerst einen Blick darauf zu werfen, woher wir kommen: die schöne, alte, natürliche Welt, welche die Menschen über zehntausende von Jahren mit ihrer einzigartigen DNA, ihrer einzigartigen Intuition und ihren einzigartigen Reflexen zu Ihrer Eigenen gemacht haben.

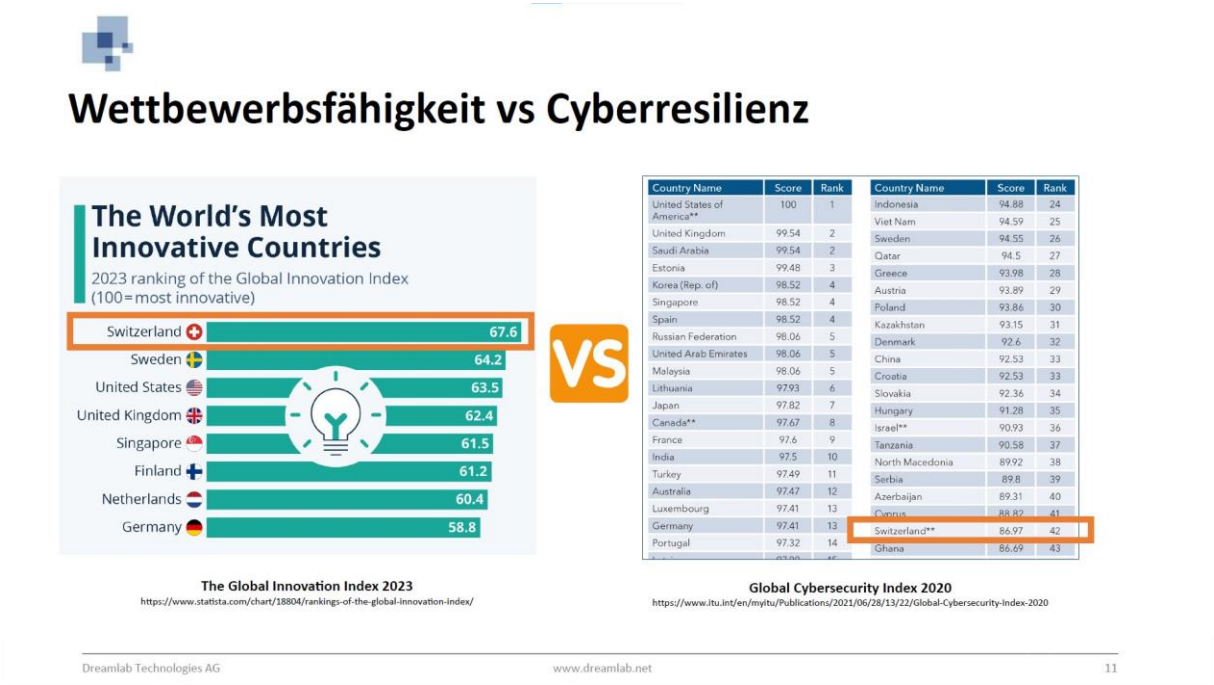
Dies sei umso erstaunlicher, da der Mensch, wenn man ihn mit den Tieren oder seinen direkten Vorfahren vergleiche, diesen in vielen Punkten unterlegen sei. Er könne beispielsweise weniger schnell rennen und weniger gut klettern. Dass sich der Mensch dennoch als dominierende Spezies durchgesetzt hat, sei neben seiner Intuition und seinen aussergewöhnlichen Reflexen noch auf zwei weitere entscheidende Vorteile zurückzuführen, die sich insbesondere in Informationsfragen bemerkbar machten: Der Mensch habe es zum einen geschafft, **Wissen zu formalisieren**, es über Generationen weiterzugeben und so über hunderttausende Jahre menschlicher Evolution einen wahnsinnigen **Schatz an Wissen und Erfahrung aufzubauen**. Daneben verfüge er auch noch über die entscheidende Fähigkeit, sich in **Gruppen ad hoc zu organisieren**. Man kenne Schwarmverhalten zwar auch in der Tierwelt, beispielsweise bei den Vögeln und Fischen. Der Unterschied sei jedoch: «Die Menschen können sich ad hoc organisieren, zweck-, ziel- und projektgebunden, um gemeinsam einen vorteilhaften Outcome zu schaffen, ob man sich nun im Voraus kennt oder nicht.» Diese Fähigkeiten hätten sich im Laufe der Evolution kumuliert und zur ersten industriellen Revolution geführt, welche in vielerlei Hinsicht den Ursprung und die Grundlage der modernen Zivilisation, der neuen Welt, dargestellt habe.

**Der Cyberraum – abstrakt, omnipräsent, gefährlich**

Der Mensch mit seiner einzigartigen Menschlichkeit habe es also geschafft, sich in den vier Dimensionen Land, Wasser, Luft und Weltraum als gewinnende Spezies zu etablieren. Die Welt 2.0, beziehungsweise die Welt, die er geschaffen hat, gehe jedoch noch weiter: so schuf der Mensch in der **dritten industriellen Revolution** einen **neuen, einzigartigen, menschengemachten Raum**: **den Cyberraum**. Die Erfindung des Computers und des Digitalraums sowie die Vernetzung über die Internettechnologie resp. weitere Netzwerktechnologien habe es ihm ermöglicht, seinen Innovationen ohne physische Limitationen freien Lauf zu lassen und Dinge anzugehen, welche in der echten Welt nicht möglich wären. Diese Entwicklungen seien geprägt gewesen von einer unglaublichen Geschwindigkeit, welche auch heute noch anhalte. Innerhalb von 50 – 70 Jahren sei der Cyberraum aufgebaut worden, und heute durchdringe und kontrolliere er die physischen Dimensionen fast vollständig. Gleichzeitig sei dieser Cyberraum für den Mensch nicht fühlbar, sinnlich nicht erreichbar. Er sei omnipräsent, unsichtbar und kontrolliere trotzdem alles. Diese Konstruktion sei einzigartig, wunderbar, schon fast paradox, aber auch brandgefährlich, weil die Gefahren und Ihre unmittelbaren Auswirkungen nicht direkt wahrnehmbar seien. Die sinnliche Wahrnehmung dafür fehle dem Menschen – oft spüre er die Auswirkungen erst, wenn es bereits viel zu spät ist. Diesen Kontext müsse man sich unbedingt vor Augen führen. Der Mensch sei Opfer seiner eigenen Innovationen. Er habe einen Raum entwickelt, der ausgesprochen mächtig sei, aber in dem seine menschlichen Attribute, seine Intuition, seine Sinnlichkeit nicht mehr griffen.

**Gefahr für den Innovationsstandort Schweiz**

Das brachte ihn zu der Schweiz im heute und hier. Er merkte an, dass die **Schweiz** laut verschiedenen Statistiken die **innovationsstärkste Nation weltweit** sei. Der Grund für ihre Innovationskraft könne einfach zusammengefasst werden: Die Schweiz könne es sich leisten und **investiere** seit vielen Jahren **systematisch in Forschung und Bildung**. Das Resultat: Die Schweiz sei heute höchst innovativ; sie habe eine starke Forschungs- und Entwicklungslandschaft; sie sei bekannt für Präzision und Qualität sowie ihre Neutralität und Unabhängigkeit. Diese Eigenschaften und Tugenden müssten jedoch auch in Zukunft sorgsam gepflegt werden.




Neben den oft doch sehr erfreulichen Statistiken und Indizes zur Schweiz würden jedoch auch Kennzahlen, die den Schweizern weit weniger Freude bereiten sollten. Der **Index** der UN-basierten **International Telecommunication Union (ITU)** umfasse ein Cyberranking betreffend die Cyber-Readiness von Nationen. Dort stehe die **Schweiz** auf dem eher mittelmäßigen **Platz 42**. Es müsse allen bewusst sein, dass dies früher oder später eine Wechselwirkung auf den Schweizer Innovationskraft haben werde. In der heutigen Welt seien Forschungsresultate letztendlich Daten, die auf Servern gehalten würden. Wenn diese Server nicht geschützt werden können, dann flössen die Resultate der Investitionen in Forschung und Entwicklung zu andere Nationen. Wie von Myriam Dunn Cavelty gehört, seien 80 % der Angriffe Spionage. Deswegen sei es wichtig auch im Bereich der Cybersicherheit mehr Sorge zu halten und ordentlicher zu arbeiten und sicher zu stellen, dass die Schweiz auch hier in eine Top-10-Position komme, um letzten Endes ihren Innovationsstandort zu schützen.

**Cyber - ein globales Risikocluster**

Beschäftige man sich mit der Bedrohungslage Cyber, dann erkenne man, dass es sich dabei um ein globales Problem handle. Gemäß dem World Economic Forum und vielen anderen Institutionen gebe es zwei große Risikocluster, die sich unserer Welt stellten: Das erste sei die Klimaverschiebung und als Nummer zwei komme dann auch schon Cyber. Dafür gebe es verschiedene Gründe. Die Gefahren, denen staatliche und auch nicht-staatliche Akteure im Cyberspace gegenüberstünden, seien von den Vorrednern bereits gut beleuchtet worden. Daneben seien die Auswirkungen davon aber auch vor allem pekuniärer Natur. Im **Jahr 2021** beliefen sich die bei Versicherern gemeldeten **Cyberschäden auf 5000 Milliarden Franken**. Das entspreche schon heute dem **BIP** der **drittgrößten Volkswirtschaft** und knapp dem **50-fachen aller Schäden durch Naturereignisse**. Das seien Schäden und Summen, die man nicht mehr einfach ignorieren könne, sondern entschiedenes Handeln nach sich ziehen müsse.

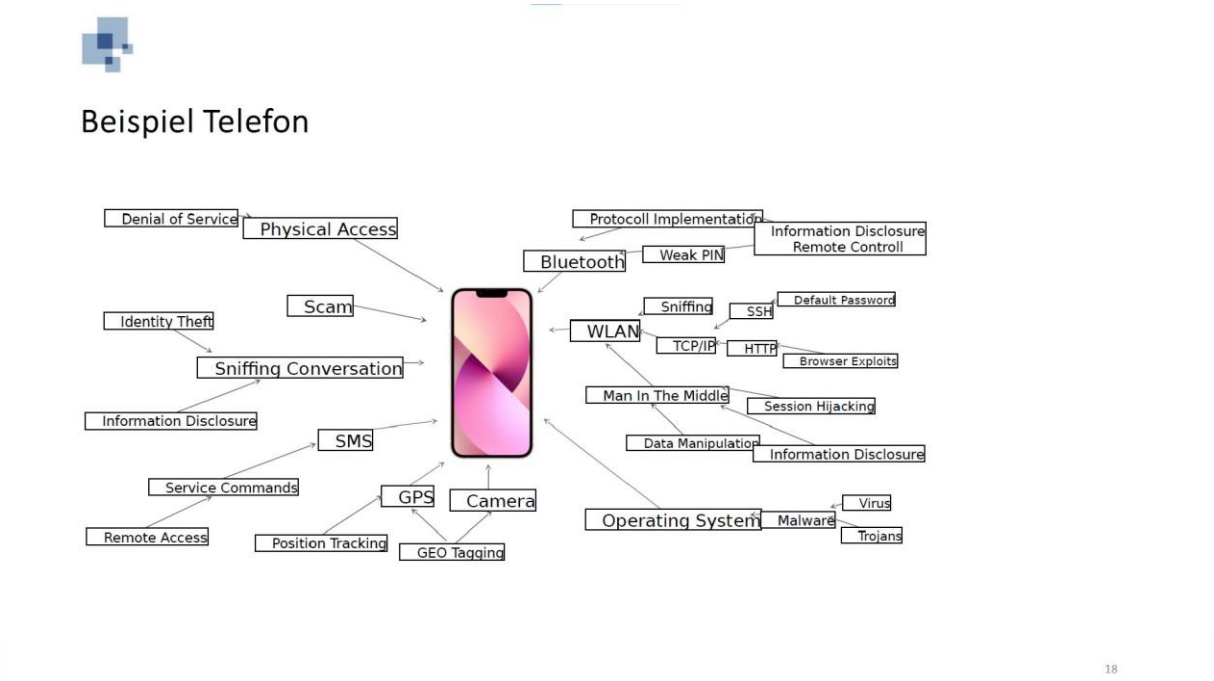
Auch die Schweiz sei davon betroffen. Auch die Schweiz sei an den Cyberraum angeschlossen und keine Insel der Glückseligen, abgegrenzt vom übrigen Cyberspace. Man gehe davon aus, dass 2021 jedes dritte Unternehmen in der Schweiz Opfer von Cyberkriminalität wurde – die Dunkelziffer dürfte jedoch noch um einiges höher sein.

**«Als Gesamtgesellschaft wird noch immer zu wenig für einen adäquaten Schutz gemacht»**

Im Zusammenhang mit dem enormen Schadensmaß durch Cyberschäden, sei ihm ein Punkt ein großes Anliegen: «Im Cyberraum hätten wir im Vergleich zu Natur- und anderen Gefahren eine größere Hebelwirkung, um uns zu schützen und könnten uns gegen Angreifer wehren.» Bei vielen Menschen fehle es jedoch nach wie vor am **Verständnis für den Cyberspace** an sich und die damit verbundenen Gefahren. Zwar habe in den letzten drei Jahren eine starke Sensibilisierung stattgefunden, dennoch werde die eigene Betroffenheit noch zu stark heruntergespielt, obwohl jedermann Ziel von Cyberangriffen werden könne. Dementsprechend tue man als Gesamtgesellschaft noch immer zu wenig, um das Problem adäquat anzugehen.

**Komplexität als Feind der Sicherheit**

Wieso der Schutz im Cyberspace jedoch überhaupt so wichtig und auch schwierig sei, könne gut anhand des Beispiels unserer Mobiltelefone aufgezeigt werden. Die ursprünglichen Mobiltelefone hätten über ein begrenztes Feature Set verfügt mit überschaubaren Möglichkeiten für Angreifer, darauf einzuwirken. Die Evolution des Mobiltelefons in ihrer unvergleichlichen Geschwindigkeit habe jedoch in den letzten Jahren dazu geführt, dass sich das Feature Set unserer Geräte fortlaufend vervielfacht habe und mit ihm auch die **Komplexität der Geräte und ihre Vulnerabilitäten**.




Vergleichbar habe sich auch die ganze IT in den letzten 20 Jahren entwickelt. Ursprünglich einfache Systeme seien in ihrer Komplexität geradezu explodiert, und **Komplexität sei bekanntlich einer der größten Feinde der Security**. Systeme mit einem solchen Komplexitätsgrad zu sichern sei äußerst schwierig. Wäre dieser Umstand in den letzten Jahren konsequenter berücksichtigt worden, hätten wir heute nicht mit diesen ungeheuren Schadenssummen zu kämpfen.

Auch in der Schweiz würden wir immer wieder Opfer, und hier solle es nicht darum gehen, mit dem Finger auf jemanden zu zeigen; stattdessen sollten solche Vorfälle Betroffenheit auslösen und Aktionen nach sich ziehen. Man müsse, von der Regierung über die Medien, die Wirtschaft bis hin zur ganzen Gesellschaft, besser werden. Überwinde man mit Tools die sinnliche Hürde des Cyberraums und mache diesen sichtbar, dann sehe man die schiere Masse an Vulnerabilitäten, welche im Cyberraum öffentlich bekannt aufzufinden seien. **«Wer die Tresortür offenlässt und draussen auf der Strasse noch ein Schild**

**hinhängt, darf nicht erstaunt sein, wenn Daten-Diebe gnadenlos zuschlagen»**, versinnbildlichte er die momentane Lage im Schweizer Cyberspace.

Eine abschließende Erklärung, wie der Cyberraum vollumfänglich gesichert, gemanagt und kontrolliert werden könnte, habe auch er nicht. Vielleicht würde es helfen, auch einfach mal innezuhalten, die ungebremste **Entwicklung der letzten 20 Jahre eingehend zu analysieren** und den C**yberraum mit dem nötigen Respekt zu behandeln**, gleich wie es auch mit dem physischen Raum gemacht werde – Dort ließe man Tresortüren schliesslich auch nicht einfach offenstehen. Und zu guter Letzt sollten damit begonnen werden, die Cyber-Dimension zu entmystifizieren und die einzigartigen menschlichen Eigenschaften darin einfliessen zu lassen.

## Referat Johann Alessandroni

Nachdem die wertvollen vorangegangenen Beiträge den Kontext der Gefahren im Cyberraum gut erfasst hatten, zeigte Johann Alessandroni auf, wie die Cybersicherheit in der Praxis ausgestaltet werden kann.

### Erkennen, nutzen, übertragen

Wenn man über die Sicherung der Informationssysteme spreche, müsse man zuerst thematisieren, wo Gefährdungen bestehen und wie man damit umgehe. Dabei reiche es nicht aus, nur die Systeme an sich zu betrachten; auch der **Faktor Mensch** müsse zwangsläufig als wichtiger Faktor berücksichtigt werden. Bei den Systemen anzusetzen und diese sicherer zu machen sei bereits eine große Herausforderung; die richtigen Stellschrauben beim Menschen zu finden und seine Verhaltensweisen anzupassen, sei jedoch noch weitaus schwieriger. Die große Bedeutung des Faktors Mensch für die Cybersicherheit werde auch durch Statistiken verdeutlicht. **74 % der Cyberangriffe im Jahr 2020** seien **an den Faktor Mensch geknüpft gewesen**. Für die Hersteller von Cybersicherheitslösungen bedeute das, dass der menschliche Faktor in den Strategien zur Sicherung von Systemen niemals vernachlässigt werden dürfe.


**Statistiken** und **Informationen** seien allgemein wichtig, um die **Gefahrenlage im Cyberraum zu verstehen**, aber noch wichtiger sei, wie man die Erkenntnisse daraus nutzen könne, um die Cybersicherheit zu verbessern. Man sehe in den Statistiken beispielsweise, dass die Angriffe in den

letzten Jahren stark zugenommen haben und dass Cyberspionage das bevorzugte Mittel auf staatlicher Ebene ist. Die Frage sei nun, wie man diese Erkenntnisse auch auf die anderen Ebenen, beispielsweise die nicht-staatliche, übertragen könne, um sich besser zu schützen. Ein weiteres Beispiel hierfür seien die Beobachtungen, welche im Ukrainekrieg gemacht werden konnten. Der physische Krieg habe im Februar 2022 begonnen. Seit September/Oktober 2021 beobachte man jedoch schon Cyberangriffe russischer Gruppen auf in der Ukraine lebenswichtige Institutionen. Der Cyberkrieg sei also schon lange in vollem Gange gewesen, bevor sich der Krieg auf dem Schlachtfeld manifestiert habe. Diese Erkenntnis verdeutliche wiederum, dass **Cyber oft schon proaktiv als Mittel genutzt werde, um Zugang zu wichtigen Informationen zu erhalten**. Dementsprechend müsse man auch in der Cyberabwehr vorausschauend handeln, um sich proaktiv zu schützen.

Die Aufgabe sei es deshalb, all diese Erkenntnisse auf die jeweiligen Ebenen und Sektoren, welche geschützt werden sollten, zu übertragen, sei es der Gesundheitssektor, die Industrie oder auch der Finanzsektor. Dabei stehe nicht nur der **initiale Schutz der Systeme im Vordergrund**, **sondern auch die Detektionsfähigkeit und die Reaktionsfähigkeit, sollte ein Angriff im Gange sein**. Die Fähigkeit, eine Kompromittierung des eigenen Informationssystems rechtzeitig zu erkennen sei elementar, um die Konsequenzen einer potenziellen Attacke zu begrenzen. Die Informationen, welche aus einer früherkannten Kompromittierung gewonnen werden können, würden wiederum dabei helfen, die eigene Früherkennung zu verbessern. Auch hier gehe es also wieder darum, Informationen zu sammeln und diese in den effektiven Schutz vor Cyberangriffen zu übertragen. Gleich verhalte es sich auch mit den Angriffen, von welchen man selber nicht direkt betroffen sei. Hier könnte man sich natürlich auch einfach zurücklehnen und sich freuen, dass man selbst verschont blieb. Zielführender sei es wiederum, die Informationen aus dem beobachteten Angriff aufzunehmen und neuerlich für die Verbesserung des Schutzes der eigenen Systeme zu verwenden.

**Proaktives, umfassendes Risikomanagement**

Diese taktischen und strategischen Informationen müssten auch verwendet werden, um das eigene Risikoassessment stetig zu überprüfen und anzupassen. Solch ein risikobasierter Ansatz werde bereits seit Jahren in vielen Bereichen auch außerhalb der Cyberwelt praktiziert. Die momentan beobachtbare Masse an Cyberangriffen im Zusammenhang mit den Kriegen in der Ukraine und in Gaza und deren Nebenschauplätzen müsse beispielsweise stets auch in die eigene Risikobewertung miteinfließen. Sei es, weil man konkrete Verbindungen zu betroffenen Akteuren pflege oder einfach, weil die Angriffe immer häufiger und schwerwiegender würden. **Das Risiko, selbst auch Opfer eines Angriffes zu werden, sei durch die Kriege eindeutig gestiegen**. Das Risikoassessment müsse also im Rahmen eines proaktiven Risikomanagements auf Basis der verfügbaren taktischen und strategischen Informationen stetig weiterentwickelt und an den Kontext angepasst werden und mit ihm auch die eigene Strategie für die Cybersicherheit.

**Elementar dabei sei wiederum, dass nicht erst gehandelt werde, wenn ein Schaden bereits eingetreten sei.** Heutzutage seien die automatisierten Lösungen für eine frühzeitige Detektion und Reaktion zwar schon sehr gut. Aber wenn diese nicht vorgängig mit den entsprechenden Inputs gefüttert werden, könnten sie ihre Wirkung auch nicht ausreichend entfalten und sich weiterentwickeln. Je besser, zuverlässiger und aktueller die Informationen seien, desto fortschrittlicher und angemessener seien die automatischen Erkennungs- und Reaktionsmöglichkeiten. Dabei müssten natürlich auch wieder die länderspezifischen Unterschiede berücksichtigt werden. Zwar könnten die meisten Informationen bis zu einem gewissen Grad universell als Inputs verwendet werden, aber die spezifischen Kontextinformationen blieben enorm wichtig, für ein an die jeweilige Organisation angepasstes Sicherheitskonzept.

**Angreifer suchen immer den Weg des leichtesten Widerstandes**

Wichtig bei der Ausgestaltung eines solchen Sicherheitskonzeptes, resp. einer Cybersicherheits-strategie, sei, wie eingangs schon erwähnt, dass man dabei **nicht nur die technologische Ebene berücksichtige, sondern einen umfassenden Schutz seiner Endpunkte anstrebe**, einschließlich des Faktors Mensch und der physischen Sicherheit der Systeme und Anlagen. Wenn man einen dieser Bereiche vernachlässige, vernachlässige man einen Faktor, der morgen einen Angriff begünstigen könnte. Angreifer suchten immer den Weg des leichtesten Widerstandes. Je mehr Verteidigungslinien für den Schutz eines Systems aufgezogen werden, desto eher würden Angreifer den Fokus auf andere Ziele legen. Sobald man also glaubhaft signalisiere, dass man a priori über eine gewisse Robustheit und Sicherheitsmaßnahmen verfüge, suchten sich Angreifer oft andere, einfachere Ziele.


**Eine Frage der Ressourcen**

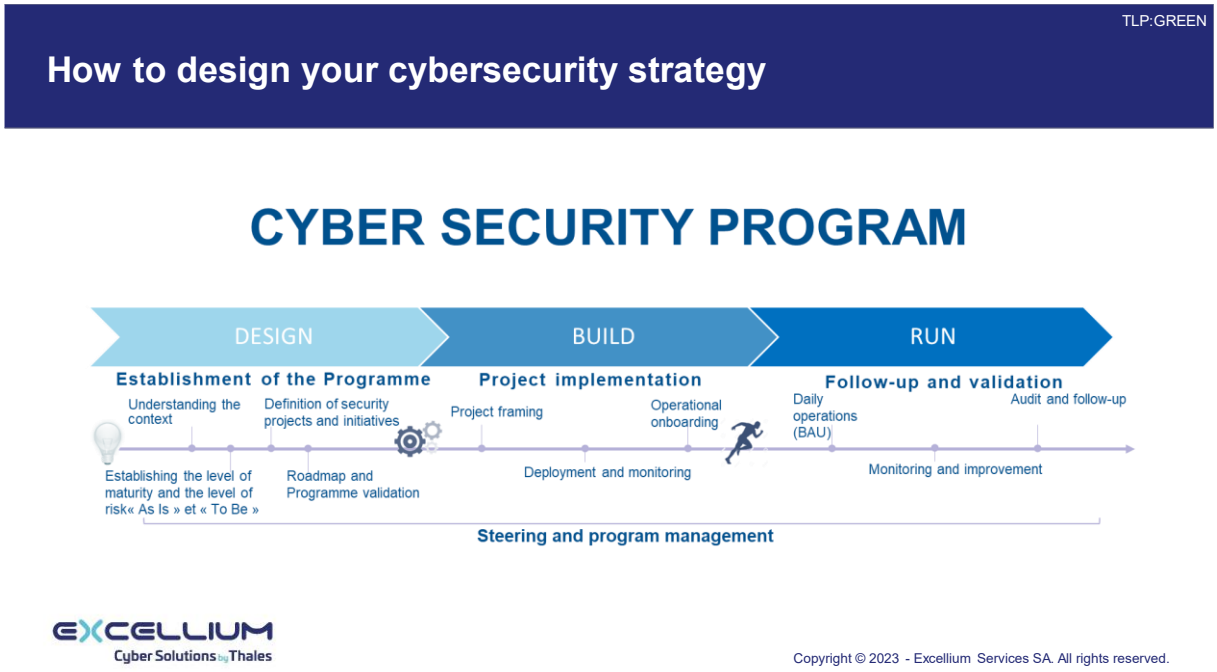
Eine wichtige Frage bei der Implementierung einer Cybersicherheitsstrategie sei auch immer, wie groß die aufgewendeten Ressourcen sein sollten. Die Ressourcen, die für die Cybersicherheit zur Verfügung stehen, seien von Organisation zu Organisation verschieden. Investitionen in die Cybersicherheit bedeuteten gleichzeitig immer auch Kürzungen des Budgets in anderen Bereichen. Glücklicherweise sei ein **grundlegender Schutz im Cyberbereich auch mit relativ wenig Aufwand schon möglich**, aber aus diesem Grund wäre es wichtig, dass man von Beginn an seine Ziele richtig definiere. Ohne Zieldefinition werde es auch nicht möglich sein, eine Sicherheitsstrategie festzulegen, die strukturiert, durchdacht und nachweisbar effektiv sei. Dabei müsse man sich auch von der Vorstellung irgendeiner einzelnen magischen Supertechnologie lösen, welche einen umfassenden Schutz bieten könne. Letzten Endes sei es immer die Gesamtheit resp. die Gesamtlogik der Maßnahmen, welche ihren Schutz ausmache.

Ein weiterer wichtiger Aspekt, den wir uns ebenfalls immer wieder in Erinnerung rufen müssten, sei die Rolle unseres Ökosystems, sprich unseres Netzwerkes an Beziehungen**. Oft seien wir nämlich nicht Herr unseres eigenen Risikos**. Die engen Vernetzungen in der heutigen Welt führten dazu, dass Angriffe

auf Partner, resp. Personen und Organisationen, mit welchen man zusammenarbeitet, auch für einen selbst ein Sicherheitsrisiko darstellen könnten. Deshalb sei es wichtig, auch mögliche Sicherheitslücken, welche in den Beziehungen zu seinen Partnern liegen könnten, genau zu beleuchten und in die eigene Strategie einfliessen zu lassen.

Wie bereits erwähnt müsse man, wenn man von Cybersicherheit spricht, sich auch überlegen, wie reagiert werden soll, wenn der schlimmste Fall eintritt. Investitionen in die Cybersicherheit dienten also nicht nur dem Schutz vor Cyberangriffen, sondern auch der Erkennung und der entsprechenden Reaktion. Hier spreche man dann von Business Continuity Management oder auch Krisenmanagement. Diese Punkte müssten in einer Sicherheitsstrategie immer prioritär berücksichtigt werden. Die Unternehmen, welche jeweils die größten Konsequenzen einer Cyberattacke zu tragen haben, seien immer diejenigen, welche diese wichtigen Punkte vernachlässigt hätten und ihren Weiterbetrieb daher auch nicht gewährleisten konnten.

**Schritt für Schritt zum effektiven Schutz**




Betrachten wir den klassischen Ablauf bei der Erarbeitung und Umsetzung einer Cybersicherheitsstrategie, dann werde in einem **ersten Schritt** üblicherweise der **Kontext definiert**. Wie bereits erwähnt, sei keine Organisation wie die andere. Man müsse den Nutzen einer Organisation, die Risiken und die Auswirkungen auf das Ökosystem verstehen, um definieren zu können, wie der Schutz im Cyberbereich ausgestaltet werden soll. Dann folge eine **Bewertung des vorhandenen Sicherheitsniveaus**, um festzustellen, wie dieses ausgestaltet ist und wo man ansetzen müsste, um die gesetzten Ziele zu erreichen. Anschließend würden die **empfohlenen Maßnahmen modelliert**. Dabei sei es wiederum wichtig, dass man den jeweiligen Mehrwert der Maßnahmen herausstreiche, damit der Fokus nicht nur auf den jeweiligen Kosten liege. Weiter müssten auch Milestones und Leistungsindikatoren definiert werden und die jeweiligen Fortschritte und Aktivitäten in regelmäßigen Bestandsaufnahmen und Sicherheitskontrollen überwacht und besprochen werden.

**Fazit**

Wie bei der Erarbeitung und Umsetzung jeder Strategie sei es auch in der Cybersicherheit wichtig, strukturiert und pragmatisch vorzugehen. Man müsse sich bewusst sein, dass es **keine magischen Lösungen gibt**. Dies bedeute auch, dass man sich auf eine **bestimmte Logik** und einen **bestimmten Ansatz** festlegen und **pragmatisch Prioritäten** setzen müsse, um die vorhandenen Ressourcen optimal zu nutzen. In diesem Zusammenhang sei es auch wichtig, sich die Logik und Struktur der gewählten Strategie und Maßnahmen immer wieder in Erinnerung zu rufen und sich darauf zurückzubesinnen, warum die gewählten Maßnahmen sinnvoll seien und welche Ziele damit erreicht werden. Auch die **Betrachtung des Ökosystems**, in dem man sich befinde, und die **stetige Überprüfung des Kontextes** helfe für ein ganzheitliches Verständnis. Und schließlich müsse man sich der **Risiken immer bewusst sein** und seine Entscheidungen darauf und die potenziellen Konsequenzen eines Angriffs abstimmen. Diese Denkweise sei elementar, um Projekte für eine Stärkung der eigenen Cyber-Resilienz aktiv anzugehen und bereit zu sein, wenn der schlimmste Fall eintreten sollte.

## Die Paneldiskussion

Nach den beiden Referaten folgte eine hochkarätige **Panel-Diskussion** moderiert durch **Fredy Müller**, Geschäftsführer des FORUMS SICHERHEIT SCHWEIZ. Neben den vier Referent:innen nahm auch **Franz Grüter** (Verwaltungsratspräsident green.ch-Gruppe; Nationalrat SVP, LU) an der Panel-Diskussion teil.


Zu Beginn wandte sich der Moderator an **Franz Grüter** und wollte wissen, ob ihn die Erkenntnisse aus den Inputreferaten erstaunen würden.

Dieser entgegnete, dass er jetzt nicht als Nationalrat spreche, sondern in seiner Funktion als Unternehmer im Rechen-Center resp. dem Data-Center-Geschäft und hier müsse man zuallererst die herausragende Rolle der Schweiz in Europa herausstreichen: **«Wir sind einer der wichtigsten Datenstandorte innerhalb von Europa, verfügen über viel Infrastruktur und beheimaten Hubs fast aller grossen Cloud-Anbieter. Von dorther sind wir natürlich auch exponiert und ein interessantes Angriffsziel.»** Neu für ihn sei die Statistik gewesen, dass die Schweiz im Cyber Security Ranking nur auf Rang 42 liegt. Er führe dies unter anderem darauf zurück, dass man sich der **Risiken im Cyberraum auch in der Politik lange Zeit nicht genügend bewusst war**. Als er 2015 in den Nationalrat gewählt wurde, habe er zusammen mit ein paar weiteren Parlamentariern erste Vorstösse zur Cybersicherheit im Parlament eingereicht und damals seien sie von vielen noch nicht richtig ernst genommen. Erst mit den grossen Zwischenfällen, welche dann ab 2018 auch in der Schweiz vermehrt auftraten, habe das Thema an Bedeutung gewonnen und ein Aufrüsten eingesetzt.

### Spionage als staatliches Mittel

Nach diesen einleitenden Worten wandte sich der Moderator **Dr. Myriam Dunn Cavelty** zu und bat sie noch näher auf die Fähigkeiten einzugehen, welche ein Staat benötigt, um erfolgreich Spionage betreiben zu können.

Darauf antwortete diese, dass das sogenannte **PETIO Framework**, was aus den Abkürzungen für People, Exploits, Toolset, Infrastructure und Organization zusammengesetzt ist, ein verbreitetes Tool

sei, welches beschreibe, welche Ressourcen für offensive Cyberaktionen benötigt werden. Früher habe man sich vorgestellt, dass eine Gruppe von Hackern in einem Keller solche Operationen durchführen könnten, dem sei jedoch nicht so. **«Es braucht wirklich spezifische, ausgeprägte Fähigkeiten und in diesem Sinn kommt es auch nicht überraschend, dass die Staaten, welche bereits über Jahrzehnte ihre Fähigkeiten im Cyberraum aufgebaut haben, auch heute diejenigen sind, welche am aktivsten sind»**, unterstrich sie die hohen Anforderungen für Spionageaktivitäten im Cyberraum.

Spionage sei schon früher ein verbreitetes Mittel gewesen. Mit dem Aufkommen des Cyberraums habe sich deren Auftreten jedoch verändert und kumuliert. Was das Auftreten dieser Gefahr in neuem Gewand für die Bundeswehr in seinem Alltag konkret bedeute, fragte der Moderator **Generalmajor Setzer.**

Es sei richtig, dass Spionageaktivitäten schon früher verbreitet waren, nur seien sie jetzt eben auch in der Dimension Cyber- und Informationsraum ein wesentliches Mittel von Staaten. Das Ziel der Spionage sei schon immer die Datengewinnung gewesen. Heute lägen diese Daten in digitaler Form auf Servern und in der Cloud und daher sei die Cyberspionage für viele ein naheliegendes Mittel.

Im Umkehrschluss sei es natürlich notwendig, dass man zum einen Schutzfunktionen einrichte, um die eigenen Systeme gegen das Eindringen von aussen zu schützen, aber auch, dass die Systeme so aufgebaut werden, dass sie im Inneren geschützt sind. **«Es kann nie ausgeschlossen sein, dass doch mal ein Angreifer in ein System eindringt, und für diesen Fall braucht man ein funktionierendes System zur Detektion und zur Reaktion»**, unterstrich Generalmajor Setzer die Notwendigkeit eines umfassenden Schutzes. Wichtig sei für sie hierbei jedoch auch, dass beim Schutz nicht einfach nur zentral vorgegangen wird. Sie seien in der Bundeswehr insgesamt, wenn man Zivile und Soldaten zusammenrechnet, etwa 270’000 Mitarbeitende. Bis zum untersten Organisationselement hätten sie Informationssicherheitsbeauftragte (ISBs) aufgestellt, sodass sie über ein breites Sensornetz verfügten. Schliesslich müsse auch noch gesagt werden, dass Cyberspionage momentan zwar weit verbreitet ist – wenn jemand aber bereits in ein Netz eingedrungen sei, dann könne Spionage irgendwann auch in Sabotage übergehen und eine Gefahr für unsere kritischen Infrastrukturen darstellen, ohne die

Schwelle eines bewaffneten Konflikts zu überschreiten. Gerne zitiere er hier sinngemäß den Militärtheoretiker Clausewitz: Es gehe im Krieg nicht darum, jemanden grundsätzlich zu zerstören, sondern es gehe darum, ihm den eigenen Willen aufzuzwingen. Wenn dazu nun also keine militärischen Mittel benötigt werden und die Kriegsschwelle nicht überschritten werden müsse, dann stellt der Cyberraum entsprechend ein probates Mittel dar, welches genutzt werde.

**Cyberattacken in verschiedenen Gewändern**

Der Moderator erwähnte, dass Cyberattacken nicht immer die Form grosser Angriffe annehmen müssen, sondern dass auch niederschwellige, wiederkehrende Attacken sehr effektiv sein könnten und wandte sich mit der Frage, ob er eine solche Aktivität ebenfalls beobachte, an **Nicolas Mayencourt**.

Dieser stimmt zu und entgegnete, dass niederschwellige Attacken sehr effektiv sein können. Gerade wenn keine Informationshygiene vorhanden sei und an vielen verschiedenen Stellen kleine Lecks existierten, dann könne ein Angreifer wertvolle Informationen über Jahre hinweg systematisch einsammeln. So könnten vollständige Informationsbilder generiert werden, ohne dass sich über grosse technische Hacks Zugriff verschaffen werden müsste. Das «Persistent» im Begriff «Advanced Persistent Threat» stehe dann auch für diese Beständigkeit und in diesem Punkt liege schliesslich auch das Differenzierungsmerkmal zur klassischen Kriminalität. Normalerweise seien Kriminelle opportunistisch und würden nicht persistent handeln, sondern vielmehr nach «einfachen» Opfer suchen. Das resultierende Fazit liess Nicolas Mayencourt folgendermassen verlauten: **«Um sich also vor Kriminellen zu schützen, muss man nicht der am besten Geschützte sein, man sollte einfach tunlichst vermeiden, am schlechtesten geschützt zu sein.»**

Darauf folgend wandte sich der Moderator an **Dr. Myriam Dunn Cavelty** mit der Frage, welche Rolle öffentlichkeitswirksame Ereignisse wie bspw. die Snowden-Affäre dabei spielten, dass die Cybersicherheit seit 2010 deutlich mehr in den Köpfen der Menschen angekommen sei.

In ihren Augen sei das Interessante diesbezüglich, dass durch die Snowden-Affäre die Nachrichtendienste das erste Mal in das öffentliche Interesse gerückt seien. Erst durch diese Aufdeckung sei bekannt geworden, dass vor allem die **Nachrichtendienste im Cyberspace aktiv seien** und entsprechende Fähigkeiten aufgebaut hätten. Ihrer Meinung nach hätten solche Ereignisse definitiv das Potenzial, das Bewusstsein der Öffentlichkeit zu formen.

**Strategic Competition**

Der Moderator wandte sich an **Generalmajor Setzer** und fragte ihn, ob er in der strategic competition, diesem Wettbewerb, dieser Machtballung unterhalb der Kriegsschwelle, auch einen Grund für den Anstieg an Cyberattacken sehe.

Generalmajor Setzer meinte, um die Frage nach dem Grund für staatliche Cyberoperationen zu stellen, müsse man immer die Frage nach der Absicht berücksichtigen. Als Beispiel könne man China heranziehen, das sich das Ziel gesetzt habe, bis spätestens 2049 in allen Bereichen die führende Weltmacht zu werden. Wenn ein Land ein solches Ziel verkünde, ordne es auch seine gesamte Strategie danach aus. Um dieses Ziel zu erreichen, benötige China nicht nur militärische Macht, sondern auch Einfluss in der Wissenschaft, der Industrie usw. Daher würden alle verfügbaren Mittel, einschließlich Cyber, genutzt, um die gesteckten Ziele zu erreichen. Es sei jedoch wichtig zu beachten, dass **die klassische Trennung zwischen staatlichen Aktionen im Cyberraum und organisierter Kriminalität heutzutage oft nicht mehr einfach durchzuführen sei.** Stattdessen beobachte man teilweise sogar Akteure, die tagsüber für den Staat und nachts auf eigene Rechnung arbeiten.

**Public Attribution**

Der Moderator leitete mit dem Vermerk, dass bereits viel über die Beweggründe für Cyberspionage und die dafür benötigten Fähigkeiten gesprochen wurde, über zum Phänomen, dass Cyberkriminelle, wenn sie denn überführt werden, öffentlich sehr intensiv genannt werden. Er wollte von **Dr. Myriam Dunn Cavelty** wissen, wieso es zu einer solchen Zurschaustellung der Täter komme.

Es gebe zwei Aspekte: Ein IT-Sicherheitselement solle verdeutlichen, dass diese Täterschaft, ihre Vorgehensweise und ihre Werkzeuge bekannt seien und aufzeigen, dass man sich schützen könne. Der zweite Aspekt beinhalte natürlich auch eine politische Komponente, die als sogenannte **Public Attribution** bezeichnet sei und erst **seit etwa rund 10 Jahren** existiere. Dies sei Teil dieser strategischen Konkurrenz und habe mit der Fähigkeit zu tun, jemanden später potenziell bestrafen zu können.

Der Moderator wollte von **Generalmajor Setzer** wissen, wie man denn effektiv im Cyberraum bestrafe und wie in der Bundeswehr zurückgeschlagen werde, wenn sie angegriffen würden.

Generalmajor Setzer entgegnete, dass das eine sehr interessante Frage sei. Das Stichwort **öffentliche Attribution** sei sehr wichtig. In Deutschland habe es bspw. über fünf Jahre gedauert, bis die Regierung den Angriff auf den Bundestag öffentlich attribuiert und den Angreifer beim Namen genannt hatte. Solche Attributionen überlege man sich aus strategischer Sicht sehr genau, aber sie böten die Möglichkeit, den Angreifern zu kommunizieren, dass **eine bestimmte Grenze erreicht worden sei**. Seine Antwort auf die Frage, was unternommen werde, wenn die Bundeswehr im Cyberraum angegriffen werde und wann die Grenze zu einem bewaffneten Konflikt überschritten sei, könne folgendermassen zusammengefasst werden. Der NATO Generalsekretär habe deutlich zum Ausdruck gebracht, dass ein Angriff in der Dimension Cyber, der in seinem Ausmaße jene einer konventionellen Attacke in einem bewaffneten Konflikt gleichkäme, mit den erforderlichen Mittel beantwortet werden würde.

Daraufhin wandte sich der Moderator an **Dr. Myriam Dunn Cavelty** mit der Frage, ob die Klassifizierung der Angriffe nach Muster, wie es die Amerikaner seit neustem pflegten, bei der Identifizierung solcher Angriffe und deren Intentionen helfe.

Diese Art von Cyberattacken zu erfassen, werde als "in Kampagnen zu denken" bezeichnet, antwortete Myriam Dunn Cavelty. Früher habe man noch in einzelnen Attacken gedacht, hätte jedoch irgendwann festgestellt, dass die Urheber solcher Attacken oft ähnliche Akteure seien. **Es sei häufig so, dass die Hintergründe hinter Attacken erst erkennbar würden, wenn Angriffe zusammen betrachtet würden, und dass sich dadurch erst ein Gesamtbild ergebe.** Aus diesem Grund sei man dazu übergegangen, kumulative Effekte anzuschauen und nicht mehr einzelne Effekte. Dadurch könne man sogar oft erkennen, dass die effektiven Konsequenzen von Angriffen noch schlimmer seien als die monetären Folgen der einzelnen Attacken, weil beispielsweise die gesammelten Informationen aus den verschiedenen Attacken kumuliert noch deutlich gefährlicher werden könnten.

**Fehlende Informationen erschweren die Lagebeurteilung**

Der Moderator richtete darauf die Frage, wie er denn die Situation für die Schweiz in diesem Kontext beurteile, an **Franz Grüter**.

Dieser begann auf seine Zeit als Präsident der aussenpolitischen Kommission zu verweisen. In diesem Amt, welches er noch bis Ende Jahr innehaben werde, waren sie mit 2 Kriegen konfrontiert, dem Ukrainekrieg und dem Krieg in Gaza. Für die Erfüllung ihrer Aufgaben würden sie teilweise Informationen des Nachrichtendienstes beziehen und auch da merke man, dass nur ein gewisser Teil der Informationen weitergegeben werde. Deswegen sei es auch für ihn schwierig, die Lage vollumfänglich zu beurteilen. Er könne somit auch für die Schweiz im Cyberspace keine abschliessende Beurteilung tätigen.


Aufgrund dieser Antwort leitete der Moderator die Frage and **Nicolas Mayencourt** weiter und wollte zusätzlich wissen, ob strategische Überlegungen zur Informationsweitergabe und zur Wahrung der Meinungshoheit in den eigenen Reihen ein Teil dieses Spiels seien.

Dieser antwortete, dass das ganz klar der Fall sei und in den letzten 10 Jahren deutlich spürbarer wurde. **Heute könne beobachtet werden, dass die Wahrnehmung den kriegerischen Verlauf systematisch mitgestalte.** Im Ukrainekrieg könne man das erste Mal perfekt inszenierte Social Media Kampagnen von beiden Seiten miterleben. Deren Einflüsse auf die Wahrnehmung können damit ganz entscheidend sein, da sie sich schlussendlich gar auf Budgetentscheide auswirken. Es sei daher ganz normal, dass wir viele Dinge in der konventionellen oder in der Cyberkriegsführung noch gar nicht wissen können, da dieses Wissen momentan noch von strategischer Relevanz sei.

An **Johann Alessandroni** wurde darauf die Frage gestellt, ob er wisse, dass Informationsflüsse häufig gefiltert oder orchestriert seien und wie er dies in seiner Arbeit wahrnehme, da er mit seiner Arbeit ja gerade die Bekanntmachung der Gefahren von Cyberangriffen verfolge.

Darauf entgegnete er, dass auch sie beobachten, dass nur bestimmte, trendige Vorfälle in der Presse respektive in den Medien zu sehen seien. Daneben würden sie jedoch einen starken Anstieg an Vorfällen beobachten, welche in der Öffentlichkeit weniger wahrgenommen würden. Es wäre aber wichtig, dass alle Angriffe öffentlich bekannt und rezipiert würden, zum einen, um den Leuten die Gefahren vor Augen zu führen, und zum anderen, weil ein umfassendes Verständnis der Angriffsmethoden, welche diesen Angriffen zugrunde liegen, auch für den Schutz der übrigen Systeme verwendet werden könnte.

**Neue Welt – alte Technologien**

Der Moderator verwiess auf ein Vorgespräch und vermerkte, dass der heutige Cyberraum eigentlich prädestiniert ist um angegriffen zu werden. Darauf fragte er **Nicolas Mayencourt**, wieso dieser Umstand nicht früher erkannt bzw. angegangen wurde.

Dieser antwortete, dass das Internet und die Informationstechnologie gebaut wurden, um Informationen zugänglich zu machen. Die Erfinder dieser Technologien wollten Informationen freisetzen und teilen. Die Situation, die er jetzt heute vorfinde, würde er fast als Success-Disaster betiteln. **Die Technologie sei so gut gewesen, dass sie die Gesellschaft so schnell adaptiert und aufgesogen habe wie ein trockener Schwamm**. Aber diese **Technologien**, weder das Internetprotokoll noch die Chips, noch die Paradigmen wie Software entwickelt wird, **seien nie mit IT-Security-Konzepten gebaut worden.** Die Gründer und Erschaffer hätten sich eine Welt, wie sie sie heute haben, nicht vorstellen können und hätten die Fundamente der heutigen Technologien auch nicht dementsprechend ausgerüstet. Was er heute sehe, sei nichts anderes als das Resultat davon, dass unreife Technologien verbaut würden und die Lücken versucht werde, mit einer Pflasterpolitik zu schließen, was jedoch nie vollständig funktionieren könne, weil die grundlegende Technologie fundamental keine Sicherheitsfeatures mitbringe. Eigentlich sollte man bei diesen Fundamenten ansetzen und diese überarbeiten, sagt zumindest der Ingenieur in ihm. Der Mensch in ihm erkenne aber auch, dass dies kaum möglich sein werde, denn die ganze Welt sei bereits ausgerüstet mit fundamental verwundbaren Technologien.

Der Moderator leitet das Thema an **Generalmajor Setzer** weiter und fragt diesen, ob die Benennung der Schwächen des Internets Thema in ihren Lehrgängen seien und wie sie mit der Thematik der sukzessiven Desasterentwicklung umgehen.

Dieser wollte eines Mal vorne wegstellen und zwar dass das Internet und die Digitalisierung sie weit nach vorne gebracht hätten. Man müsse jetzt auch aufpassen, dass man nicht das Kind mit dem Bad ausschüttet. Sie erkennen momentan sukzessive, dass alles zwei Seiten habe. Man sollte jedoch auch nicht plötzlich alles zurückschrauben. In diesem Wettkampf, von dem gesprochen werde, werde derjenige zumindest gleich lange bestehen wie die anderen, der technologisch gesehen spitze bleibe. Er bediente sich hierzu dem gängigen Beispiel der KI. KI sei eine neue Software mit neuen

Möglichkeiten. Diese werde man nutzen, man nutze sie bereits. Die KI beinhalte Gefahren, aber genauso könne sie im Hinblick auf Informationssicherheit und den Schutz des Systems helfen. Entsprechend könne man KI dazu nutzen, um das System resilienter zu machen, da diese in der Lage sei, Anomalien im System viel schneller zu erkennen, als das jeder Mensch könne. In der Entwicklung liege der Fokus dementsprechend nicht nur auf "Fight the problem", unter dem Gesichtspunkt, dass alles schlecht sei, was sie haben, sondern hauptsächlich darauf, wie Bestehendes verbessert werden könne. Hierzu nennt er drei Stichworte. Das eine sei für zukünftige Systeme "**Security by Design**", sodass Sicherheitscode von Anfang an inkludiert sein werde. Zweitens müsse man die Menschen, die damit umgehen, schulen, sodass sie zweckmässig damit umgehen könnten, insbesondere unter dem Gesichtspunkt "**Social Engineering**". Und das Dritte, und das sei die grösste Herausforderung, sei, dass sie für die "**Legacy-Systeme**" Verfahren schaffen, um deren Verwundbarkeiten zu beheben. Diese sollten möglichst durch adäquate, zukünftige Systeme ersetzt werden. Aber seine Philosophie sei, nicht den Kopf in den Sand zu stecken, sondern die Digitalisierung und die Sicherheit weiterhin an der Spitze voranzutreiben.

**Analogisierung statt Digitalisierung?**

Der Moderator hakt hier nach und stellt die Frage an **Nicolas Mayencourt**, ob es denn nicht besser wäre, wenn wir uns weniger in der digitalen Welt aufhalten würden und wieder vermehrt analog unterwegs wären und dadurch weniger auf die Verarbeitung von Big Data durch KI angewiesen wären. Mit leicht ironischem Touch fragte der Moderator, ob es denn nicht besser sei, wenn man seine Passwörter wieder auf einen Zettel aufschreibe als diese im Internet zu speichern.

Darauf entgegnete Nicolas Mayencourt, dass eine Grundregel existiere, welche folgendermassen lautet: **«Wer nicht mit der Zeit geht, geht mit der Zeit.»** Die Digitalisierung sei hier, um zu bleiben, und sie bringe ganz viele gute Dinge mit sich. Das könne er nur unterschreiben. Es gebe ganz, ganz viele positive Aspekte. Sein Votum an dieser Stelle wäre, aufzuhören, naiv zu sein. Man solle der Digitalisierung und dem Cyberraum die notwendige Ernsthaftigkeit geben und diese mit dem notwendigen Respekt betrachten. Ein Betriebssystem für ein Atomkraftwerk in Betracht zu ziehen, wo in der Lizenzvereinbarung stehe "not fit for any purpose" und jegliche Haftung ausgeschlossen werde, sei schlicht und ergreifend grundsätzlich falsch. Das könne ja nicht der Sinn der Sache sein. Genau dort solle man ansetzen und sich vielleicht nicht nur fragen, was man tun könne, sondern auch ob es sinnvoll sei und wie man es sinnvoll tun könne. Damit wolle er sagen: ja nicht aufhören, aber kontrollierter und besser vorgehen.

**Internationales Regelwerk**

Der Moderator ging nach dieser Antwort auf das erwähnte Anregung ein, dass ein internationales Regelwerk geschaffen werden könnte und fragte **Dr. Myriam Dunn Cavelty**, ob das ein Thema sei, welches weiterhin Zukunft habe.

Diese erwidert, dass das ganz klar der Fall sei und dass es auf verschiedenen Ebenen bereits **Normen und Regeln** gäbe, beispielsweise in der **NATO** oder in der **UNO**. Natürlich würden auch Regulationen besprochen, in der EU und auch bei uns gebe es bereits solche. In den USA zeichne sich seit diesem Jahr zudem ganz klar ab, dass man auf verstärkte Regulationen im IT-Sektor setzten möchte. Sie meinte zudem, dass man nicht alles regulieren müsse, bei der nachträglichen Implementierung müsse jedoch mit Köpfen vorgegangen werden. Sie glaube aber, dass wir das schon hinkriegen werden, wenn denn der Wille da sein sollte.

**Nicolas Mayencourt** ergänzte dazu, dass wir da schon einmal gewesen seien. Als veranschaulichendes Beispiel zeigte er **die Entwicklung des Autos** auf, zu welcher einige Parallelen gezogen werden können. Denn bei diesen existierten vorerst keine Gurte, aufgrund der Häufung von schweren Unfällen wurde

mit der Zeit jedoch ein ganzes Sicherheitsregelwerk aufgebaut, weswegen wir heute Gurte, Airbags und Führerausweis hätten. Durch dieses System sei das Ausmass der Schäden soweit reduziert worden, dass es sich heute in einem akzeptablen Rahmen befinde. Zusätzlich gebe es die internationale Kommunikationsunion, ohne welche heute kein Telefonnetz existieren würde. Dort seien auch ganz viele Dinge sehr gut geregelt. Beim Internet sei jedoch lange die Haltung vertreten worden, dass man dieses sowieso nicht kontrollieren könnte, was falsch gewesen war und noch immer sei. Die Möglichkeiten dazu existierten bereits, wir hätten auch die notwendigen Organisationen, wir müssten diese einfach einsetzen.

Gegen Schluss wendet sich der Moderator nochmals mit einer Frage an **Franz Grüter**. Er wollte von ihm wissen, ob seiner Einschätzung nach die Entwicklung eines Cyberrates in Genf, wodurch die Schweiz diesbezüglich eine führende Rolle übernehmen könnte, realistisch erschein.

Er sagte, dass er zwei mögliche Initiativen sehe. Im ersten Fall sei ihnen leider Luxemburg zuvor gekommen, indem sie eine **E-Embassy** entwickelt hätten. Das sei vergleichbar mit einem internationalen Flughafen, wo internationales Recht gelte. Dort lagerten beispielsweise das **IKRK**, das Internationale Komitee vom Roten Kreuz, **seine hochsensitiven Daten**. Deren Daten seien somit in einen nichtstaatlichen, internationalen Raum disloziert. Die Daten seien heute in Luxemburg. Auch Estland habe nach dem russischen Cyberangriff 2007 eine komplette Zweitinfrastruktur in Luxemburg aufgebaut. Das hätten sie als Schweiz seiner Meinung nach verschlafen. Sie könnten es wahrscheinlich noch immer aufbauen, denn seiner Meinung nach würde ein ähnlicher, digitaler Raum sehr gut zu Genf passen.

Der Moderator fragte hier nach, inwiefern die einzigartige Topographie der Schweiz und damit verbundenen Bauwerke wie beispielsweise der Gotthard-Tunnel einen Vorteil bringen könnten, indem man dort Datencenter etablieren könnte.

Darauf antwortete **Franz Grüter**, dass es durchaus Beispiele gebe, wo man Rechenzentren in Bunkern errichtet habe. Er freue sich immer über diese Projekte, weil sie dem **Nimbus als Datenbunker Schweiz**

helfen würden. In der Realität seien die Risiken für die gelagerten Daten nicht physisch Natur, es seien keine klassischen Einbrecher, die dort einen Surfer klauen würden, sondern es handle sich um Hackerangriffe. Gegen solche sei ein Rechencenter in einem Bunker genauso schlecht oder gut geschützt wie in einem herkömmlichen Datacenter.

**Publikumsfragen**

Zum Schluss öffnete der Moderator die Fragerunde für das Publikum.

Darauf meldete sich **Adrian Marti** zu Wort, welcher bei der Firma Ereneos arbeite. Er meinte, dass sie selber Berater für Informationssicherheit bei grossen Organisationen seien. In seinen Augen sei das Wichtigste, dass Sicherheit zu einer **Grassroot-Bewegung** werde und wollte von den Speaker:innen wissen, wie man dieses Ziel erreichen könnte.

Der Moderator, sichtlich erfreut aber der Frage, meinte, dass das seine Abschlussfrage gewesen wäre, Adrian Marti ihm nun aber zuvorgekommen sei. Er wandte sich daher mit der Frage, wie man den das Sicherheitsbewusstsein allgemein schärfen könne, an die Panelisten.

**Nicolas Mayencourt** entgegnete, dass er glaube, dass wir so etwas wie ein **Update unseres Gesellschaftsvertrags** bräuchten, weil dafür so etwas wie ein «Mindupdate» von uns allen notwendig sein würde. **Sicherheit sei grundsätzlich ein Teamsport**, der uns alle brauche, ansonsten werde es nicht funktionieren. Daher solle über die Rollen, Rechte und Pflichten jeder Organisation gesprochen werden. Es müsse sich gefragt werden, was Herr und Frau Schweizer machen, was die Wirtschaft mache, was die Forschung mache, was der Staat mache, was das Militär mache – und die allerwichtigsten Fragen, welche gestellt werden müssten, seien, wie man Grenzschutz heute kenne und ob man etwas ähnliches im Cyberraum auch bräuchte. Damit spielte er den Ball dem Vertretern aus der Politik zu.

Der Moderator tätigte die Überleitung und richtete die Frage, wie wir resilienter und sicherheitsbewusster werden können, an **Franz Grüter**.

Wie bereits erwähnt wurde, war er kürzlich im Baltikum und auch in Israel, bevor der Krieg ausbrach. Dort äußern die Leute häufig, dass aufgrund des bestehenden, langjährigen Friedens manchmal eine gewisse „**Naivität" in der Schweiz** bestehe. Es sei uns manchmal zu wenig bewusst, was in der Welt wirklich vorgehe. Trotz allem könne hier zum Schluss eine positive Bilanz gezogen werden; ein Umdenken habe stattgefunden. Es sei nicht bekannt, ob vor acht oder zehn Jahren so viele Leute zu einem solchen Thema wie heute hier versammelt werden hätten können. Heute sei man sich dem jedoch bewusster geworden und die Unternehmen tätigten große Bemühungen, würden beispielsweise Spezialisten engagieren, welche sie beraten, und auch beim Staat habe es Fortschritte gegeben. Beim Bund werde im nächsten Jahr beispielsweise das Bundesamt für Cybersicherheit gegründet.

Für das Schlusswort wandte sich der Moderator noch einmal an **Generalmajor Setzer** und wollte von ihm wissen, wie er denn spüre, dass die Bevölkerung, aber vor allem auch junge Leute, sicherheitsaffiner geworden seien.

Dieser merkte an, dass die Jugend vermutlich viel besser mit der Digitalisierung umgehe als es bei seiner Generation noch der Fall gewesen sei. Es bestehe jedoch auch bei der Jugend ein Bedarf, der derzeit noch zu kurz komme. Es müsse auch in Bildungseinrichtungen Sensibilisierung geschaffen werden. Dies sei aus seiner Sicht etwas, was noch gesteigert werden müsse, da Sicherheit, wie bereits vorgängig erwähnt, ein Teamsport sei, der beim Einzelnen beginne. **Cyberangriffe setzen zumeist beim schwächsten Glied der Kette an**. Daher sei Digitalisierung und Cyber Sicherheit keine Angelegenheit, um die sich nur einige Wenige kümmern müssten, sondern sie gehe alle an. In diesem Zusammenhang könne die Unterstützung der vorgeschlagenen Awareness-Tage nur befürwortet werden.

Zu guter Letzt richtete der Moderator die Abschlussfrage an **Dr. Myriam Dunn Cavelty**.

Sie gab zu verstehen, dass sie eigentlich das, was der Herr General gesagt hatte, habe mitteilen wollen: **Bildung und Ausbildung seien auf jeden Fall erforderlich und notwendig**. Sie würde sich zudem auch wünschen, dass Menschen, die vor Technologie Angst hätten, diese Angst ablegen und erkennen könnten, dass es auch in ihren Händen liege, da das System ein von Menschen geschaffenes System sei, was bedeute, dass es auch verändert werden könne. Hierfür müssten die Menschen jedoch ihre Angst überwinden. Es handle sich im Allgemeinen um ein sehr menschliches Thema, und sie würde sich wünschen, dass den Menschen in Zukunft mehr Handlungswillen in diesem Bereich vermittelt werde.

Damit war die Paneldiskussion abgeschlossen und der Moderator dankte dem Publikum für seine Aufmerksamkeit und den Panelisten für das interessante Gespräch.


**FORUM SICHERHEIT SCHWEIZ**

c/o MUELLER Consulting & Partner
Gemeindestrasse 48
CH-8032 Zürich

Phone +41 44 533 04 00
sekretariat@forum-sicherheit-schweiz.ch