Fake News und digitale Sicherheit in offenen Gesellschaften

Fazitbericht | 7. FSS Security Talk vom 1. Oktober 2020, Universität St. Gallen

Irreführende Zeitungsberichte, Falschmeldungen im Internet, Desinformations-Kampagnen in sozialen Medien, Fake News-Attacken auf Personen, Unternehmen, Organisationen, Regierungen und Länder stellen eine ernsthafte Gefahr dar für offene Gesellschaften und Demokratien. Nicht überreagieren, aber mit Eigenverantwortung und Medienkompetenz das Problem bekämpfen, forderten die Referierenden am 7. FSS Security Talk.

Rund 100 Entscheidungsträger, Studenten und Interessierte fanden sich an der Universität St. Gallen zum 7. FSS Security Talk ein, der vom FORUM SICHERHEIT SCHWEIZ (FSS) zusammen mit dem Sicherheitspolitischen Forum (spf) St. Gallen organisiert wurde. **Stadtpräsident Thomas Scheitlin** begrüsste zum Auftakt der Veranstaltung die Referierenden und Gäste. Die St. Galler seien sehr stolz auf die Universität St. Gallen, betonte er, denn sie sei ein bedeutender Erfolgsfaktor für den **Bildungs- und Forschungsstandort St. Gallen**. Weitere Erfolgsfaktoren seien das IT-Cluster «IT St. Gallen Rockt», welches 90 Unternehmen, 16 Bildungspartner und 35 Netzwerkpartner vereinigt oder der geplante Innovationspark im Westen der Stadt. «Fake News oder nicht?» - Nein, meinte Scheitlin, seine Aussagen seien wahr und nachprüfbar. Wirkliche Fake News jedoch träfen gerade den Mann oder die Frau auf der Strasse, wenn Medien und Politik einen Vertrauensverlust erleiden. Dabei seien **Fake News nichts Neues**, wie Scheitlin abschliessend festhielt, aber die Art und Geschwindigkeit ihrer Verbreitung habe sich verändert.

Ein globales Buffet von Falschinformationen

Im ersten Keynote-Referat ging **Jürg Bühler**, Vizedirektor des Nachrichtendienstes des Bundes (NDB), auf die NDB-Tätigkeiten in Bezug auf Fake News und **Beeinflussungsoperationen** ein. Bühler betonte einleitend, der NDB sei nur für einen Teil des Problems zuständig – **Beeinflussungsoperation** ausländischer staatlicher Akteure, welche sich gegen das Funktionieren der Schweiz und ihrer Gesellschaft richten. In der Schweiz bearbeite der NDB diese Phänomene grundsätzlich nicht, ausser es gebe klare Anzeichen, dass ein ausländischer Nachrichtendienst in der Schweiz tätig wird. Falschinformationen sind **kein neues Phänomen**, wie Jürg Bühler ebenfalls betonte, der **Informationsraum** ist schon lange **Teil von Konflikten**. Zu wissen, welche Informationen wahr sind, bleibe aber essenziell für die autonome Entscheidungsfindung der Schweiz, und daher ein Kernanliegen des NDB.

Der Effekt von Beeinflussungsoperationen ist nur schwer messbar, gerade weil die Reaktionen der Zielgruppen nur schwer vorhersehbar sind. Viele Beeinflussungsoperationen wollen kein bestimmtes Narrativ verbreiten, sondern möglichst viel **Verwirrung stiften,** damit die

Wahrheit vergessen geht. Diese Methode sei sowohl beim Attentat auf den ehemaligen russischen Spion **Sergej Skripal** in Salisbury als auch der Vergiftung des Oppositionellen **Alexei Nawalny** angewandt worden**.** Der NDB habe bisher hingegen **keine Anzeichen für die Beeinflussung von Wahlen in der Schweiz** feststellen können. Wahrscheinlich sei die Schweiz international nicht wichtig genug, vermutete Jürg Bühler, gleichzeitig würden aber auch die dezentrale Organisation und das Mehrparteiensystem der Schweiz zum Schutz beitragen. Bühler führte weiter aus, die Digitalisierung verstärke die Verbreitung von Fake News: «Was früher der Stammtisch war, ist heute ein **globales Buffet**, von dem jeder etwas nehmen, aber auch etwas hinstellen kann». Daher müssten wir als gesamte Gesellschaft dafür sorgen, das Problem kleinzuhalten.

Die Wahrheit als solches gibt es nicht

Dr. Myriam Dunn-Cavelty, leitende Dozentin für Sicherheitsstudien und Stellvertreterin für Forschung und Lehre am Center for Security Studies, betonte im zweiten Keynote-Referat, man müsse zwischen **zwei Bedeutungen von «Fake News»** unterscheiden. Einerseits meinen «Fake News» **gezielte, faktenverzerrte Falschnachrichten**, die sich durch Faktenchecks identifizieren lassen. Andererseits wird der Begriff «Fake News», frei nach Donald Trump, zur Diskreditierung der Medien verwendet. Diese Art von Fake News entstehe aus dem **Zusammenspiel unterschiedlicher Wahrheiten**, gerade wenn im Zeitalter postfaktischer Tendenzen Menschen lieber ihren Gefühlen als Fakten glauben.

Quelle: Präsentation Dr. Myriam Dunn-Cavelty

Auch Dr. Myriam Dunn-Cavelty hielt fest, **gezielte Falschinformationen** seien **nichts Neues**. Es habe in der Gesellschaft immer **unterschiedliche Wahrheiten** gegeben und das sei auch gut so. Auch die politische Ausnutzung des Wissens um deren Existenz ist nichts Neues, aber mit der Zeit verkamen diese Tendenzen zu Subkulturen. Heute werden diese Subkulturen wieder präsenter und Verschwörungstheorien zunehmend politisch instrumentalisiert. **Technologie sei nicht der Auslöser dieses Phänomens**, wohl aber ein Verstärker, erläuterte Dr. Myriam Dunn-Cavelty als zweites. Wir erfahren heute vieles, was wichtig ist auf der Welt, nicht mehr am eigenen Leib und somit nachvollziehbar, sondern nur noch durch «die Medien». Weil wir zunehmend ausländische, insbesondere amerikanische Medien konsumieren, entsteht so eine einseitige **globale Awareness für Probleme**. Gleichzeitig hat sich die Medienlandschaft stark verkleinert. Es fehlen heute **«Circuit Breaker»**, Journalisten, welche in die Tiefe gehen, und Falschnachrichten potenziell identifizieren und deren Verbreitung stoppen können. Stattdessen werden **Algorithmen** eingesetzt, welche die Verbreitung von Fake News weiter beschleunigen.

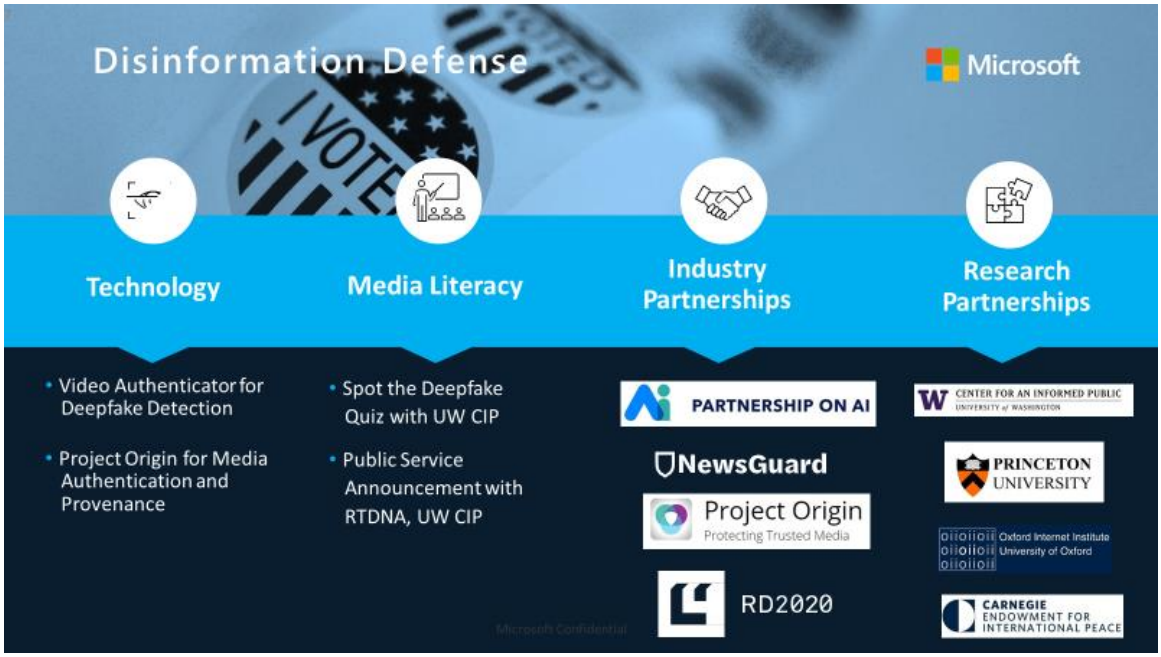
Jedoch ist **Problem in der Schweiz sehr klein**, meinte Dr. Myriam Dunn Cavelty. Als Gesellschaft sollten wir keinesfalls überreagieren, sonst spiele man den destabilisierenden Zielen von Fake News in die Hände. Zu dieser potenziellen Überreaktion trage bei, dass die **Rolle von Technologien** stets **überbewertet** würden. Fake News sollte daher nicht nur als theoretische Debatte geführt werden. Es brauche Studien dazu, ob in der Schweiz tatsächlich ein Effekt von Fake News zu sehen sei. Hier stehe die **Wissenschaft** aber **erst am Anfang**. Abschliessend hielt Dr. Myriam Dunn-Cavelty erneut fest, dass es **die Wahrheit als solches nicht gibt**. Daher könne auch **keine Instanz Wahrheit definieren.** Stattdessen forderte sie, dass die Gesellschaft angesichts der Existenz unterschiedlicher Wahrheiten **Resilienz**, die Fähigkeit Bedrohungen standzuhalten, aufbaut.

Geteilte Verantwortung für die Entwicklung eines nachhaltigen digitalen Raums

Welche Verantwortung tragen Markt und Staat für Fake News und digitale Sicherheit? – Darauf ging **Dr. Ladina Caduff**, Director Corporate Affairs bei Microsoft Switzerland, im dritten Keynote-Referat ein. Einleitend betonte Dr. Caduff, die **Welt sei vernetzter als je zuvor**. Bis 2030 werden 50 Milliarden verbundene Geräte erwartet und 15 – 25% der globalen Wertschöpfung wird bereits heute durch die Datenwirtschaft generiert. Damit neue Technologien

wertschöpfend eingesetzt werden können, brauche es jedoch **Medienkompetenz** und **Tech Capability**, d.h. die Beurteilungsfähigkeit des Einzelnen, aber auch der Politik, was Technologien können und nicht können. Der entscheidende Faktor für die erfolgreiche Anwendung neuer Technologien sei jedoch **Vertrauen** – in Produkte, in Anbieter und in den digitalen Raum**.**

Jedoch lasse sich in Bezug auf die Bedrohungslage eine Verschiebung von Cyberkriminalität hin zu **Cyber Warfare** beobachten, hielt Dr. Ladina Caduff fest. Das Ausmass, die Ausgereiftheit und die Breite der Auswirkungen nationalstaatlich motivierter Attacken im Cyberspace habe klar zugenommen. Im Vergleich zur konventionellen Kriegsführung ergeben sich jedoch bedeutende Unterschiede. Der digitale Raum entzieht sich den Grenzen nationaler und internationaler Rechtsprechung. Es fehlt eine **«digitale» Genfer Konvention**, welche die Zivilbevölkerung bei kriegerischen Auseinandersetzungen schützen würde. Andererseits wird der digitale Raum in erster Linie durch private Unternehmen betrieben und gesichert. Tech-Firmen wie Microsoft sind daher die **First-Responder bei Cyber-Attacken**.



Quelle: Präsentation Dr. Ladina Caduff

Im Bewusstsein um diese Rolle hat Microsoft das **Defending Democracy Program** lanciert, welches auf drei Pfeilern beruht: Integrität von Wahlprozessen, Kampagnensicherheit und **Disinformation Defence**. Um mit Falschinformationen umzugehen, betonte Dr. Ladina Caduff, gebe es einerseits technologische Mittel, z.B. Tools um Deep Fakes zu erkennen. Andererseits brauche es **Medienkompetenz**, weshalb Microsoft Individuen und politische Parteien im Umgang mit Informationen schult. Jedoch könne auch Microsoft nur beschränkt wirksam sein, wenn es nicht Partnerschaften mit anderen Unternehmen eingeht. Ein Beispiel dafür ist der **Cybersecurity Tech Accord**, in dem sich mehr als 30 internationale Unternehmen verpflichten, in Cybersicherheit zu investieren. Um das Problem der Normierung des digitalen Raums anzugehen braucht es jedoch **Multi-Stakeholder Dialoge** wie den **Paris Call for Trust and Security in Cyberspace,** welche Unternehmen, Staaten und Zivilgesellschaft zusammenbringen. Denn,

so betonte Dr. Ladina Caduff abschliessend, es liege im Interesse von uns allen, den **digitalen Raum so stabil wie möglich** und für **nachfolgende Generationen nachhaltig** zu gestalten.

Die digitale Welt transparenter machen

Anschliessend wandte sich **Vera Jourova**, Vize-Präsidentin der Europäische Kommission für Werte und Transparenz, mit einer **Videobotschaft** ans Publikum. Die Covid-19 Krise habe gezeigt, wie stark wir von Technologie abhängig sind. Daher müssen wir heute die richtigen Entscheidungen treffen, um sicherzustellen, dass Technologie auch in Zukunft uns dient. Denn Technologie schafft auch Risiken für unsere Sicherheit und unsere Demokratie. Dies habe die «**Infodemie»** während der Covid-19 Pandemie gezeigt, der Überfluss an Informationen über das Virus. Das Problem werde verschärft durch in- und ausländische Akteure, die Technologie als Waffen missbrauchten, so Vera Jourova. Aus Sicht der Europäische Kommission sei daher der Moment gekommen, um zu handeln und die **digitale Welt transparenter zu machen**. Der **Digital Services Act** solle Plattformen dazu anhalten, verantwortungsbewusst zu handeln, besonders in Bezug auf illegale Inhalte, und eine Fragmentierung des digitalen Binnenmarktes verhindern. Gleichzeitig arbeite die Kommission an Lösungen, um den **digitalen Raum transparenter** zu machen und die **Cybersicherheit in der Union** zu erhöhen.

Fake News und digitale Sicherheit – wie gross ist das Problem?

Zur Panel-Diskussion begrüsste **Moderator Fredy Müller**, Geschäftsführer des FORUMS SICHERHEIT SCHWEIZ, zusätzlich zu den drei Referierenden **Anne-Marie Buzatu**, Senior Advisor bei der ICT4Peace Foundation, und **Hernâni Marques**, Vorstandsmitglied des Chaos Computer Club Schweiz. Angesprochen auf die Initiativen der Europäischen Kommission, meinte **Anne-Marie Buzatu**, diese seien der **Start einer Konversation** über die Normierung des digitalen Raums. Transparenz und Wissen, woher Quellen im digitalen Raum kommen, seien entscheidend.

Jürg Bühler stellte fest, dass sich die Tonalität von Cyberangriffen und Desinformationen **in den letzten Jahren verschärft hat**, auch wenn es staatliche Angriffe im digitalen Raum schon immer gab. Dies sei jedoch Ausdruck der allgemeinen internationalen Spannungssituation. Aus Sicht der Wissenschaft sei es sehr schwer den **Effekt von Fake News** festzumachen, betonte **Dr. Myriam Dunn-Cavelty**. Das Center for Security Studies habe jedoch ein Projekt in der Ukraine, wo man Fake News während der bevorstehenden Wahlen live beobachten will. Anschliessend sollen die Probanden in Panel-Diskussion befragt werden, ob und welche Faktoren einen Unterschied gemacht haben.

Hernâni Marques kritisierte die Praxis internationaler Tech-Firmen massenhaft **Daten zu sammeln**. Es lägen heute so viele Daten über uns vor, führte er aus, dass wir gezielt mit Informationen angegangen werden könnten. Diese Firmen müssten aus seiner Sicht dringend gebändigt werden. Für Microsoft sei die Frage nach der **Monopolstellung bei Plattform-Thematiken** ein Spannungsfeld, mit dem man sehr sorgfältig umgehe, antwortete **Dr. Ladina Caduff**. Anders als Facebook oder Twitter sei Microsoft aber ein Datenprozessor. **Datenschutz und Schutz der Privatsphäre** sind zudem eine **geteilte Verantwortung**, betonte Dr. Ladina Caduff. Microsoft tue vieles, um seine Produkte sicherer zu machen, aber auch die Kunden würden eine Teilverantwortung tragen. Microsoft sehe, dass die **Vertrauensfrage essenziell sei,** sonst würden die Kunden Technologie nicht mehr anwenden.

Die Folgen von Cyberattacken auf kritische Infrastrukturen

Welche Folgen eine Cyberattacke auf kritische Infrastrukturen haben kann, zeigt **Wannacry**: In britischen Spitälern mussten **ca. 90'000 Operationen verschoben** werden, weil Spital-Computer gehackt wurden. **Hernâni Marques** erläuterte, Wannacry sei durch eine dahinterliegende Sicherheitslücke verursacht worden, welche von der NSA entwickelt, aber anschliessend geleakt wurde. Microsoft habe von der Sicherheitslücke gewusst, aber sie unter

Verschluss gehalten. Hernani Marques kritisierte diese **Hortung von Sicherheitslücken** durch staatliche Nachrichtendienste. Dies würde, das **Vertrauen in IT-Systeme gefährden**. Er forderte, Europa müsse eigene, transparente IT-Systeme entwickeln. **Dr. Myriam Dunn-Cavelty** ergänzte, das Internet sei nie für hochsichere Prozesse gebaut worden. Die Tendenz, dass staatliche Akteure gefährliche Verwundbarkeiten kennen, aber nicht veröffentlichen, weil sie solche Sicherheitslücken strategisch nutzen wollen, könne nicht einfach gelöst werden. Gerade deshalb brauche es **Resilienz**. Auch **Dr. Ladina Caduff** betonte, es gebe **keine Null-Risiko-Gesellschaft**. Microsoft sage seinen Kunden daher immer: «Assume breach!».

Eine Attacke wie Wannacry, die auch Spitäler angreift, käme im zwischenstaatlichen Bereich einem **Tabubruch** gleich, betonte **Jürg Bühler.** Unerfreulicherweise stehen solche Mittel aber auch privaten Akteuren zur Verfügung. Jürg Bühler stellte die These in den Raum, dass Produkte wohl weniger innovativ, aber sicherer wären, wenn **Software-Hersteller** ähnlich **strenge Haftungsregeln** eingehen müssten wie in anderen Bereichen. **Hernâni Marques** bekräftigte, Produkthaftpflichten einzuführen wäre sicher ein Teil der Lösung. Gerade bei autonomen Fahrzeugen könnten Manipulationen von Produkten fatale Folgen haben. Produkte müssten daher so sicher gemacht werden, dass sich der **Aufwand nicht lohnt, sie zu hacken**.

Hernâni Marques kritisierte zudem den **Digitalisierungswahn**. Es brauche nicht überall Digitalisierung, manche Systeme, wie z.B. AKWs, müssen vom Netz getrennt werden. Sonst werde das Internet of Things zu einem **«Internet of Terror». Dr. Ladina Caduff** betonte, schlussendlich müssten Gesellschaften in Aushandlungsprozessen entscheiden, wie sie mit Technologie umgehen wollen. Microsoft habe aber in seinem kürzlich zum ersten Mal publizierten **Cyber Defense Report** ebenfalls festgestellt, dass **Angriffe auf Internet-of-Things-Geräte** im letzten Jahr um **mehr als 35% gestiegen** sind. Auch ICT4Peace versuche Herausforderungen wie das autonome Fahren weit vor dem Rest der internationalen Gemeinschaft zu erkennen, erklärte **Anne-Marie Buzatu**. Sie forderte, über **Lösungen nachzudenken, bevor Unfälle passieren**.

Fake News in der Schweiz: Hype oder Realität?

Fredy Müller lenkte die Aufmerksamkeit der Panellisten anschliessend auf die Frage des Umgangs mit Fake-News Phänomenen in der Schweiz. Durch den Konsum von Medien aus den USA werden wir gezwungen, den Spagat zwischen amerikanischen und Schweizer Nachrichten zu schaffen. **Dr. Myriam Dunn-Cavelty** griff diesen Punkt aus ihrem Keynote Referat auf: Es gehöre zu modernen Gesellschaften, dass wir **überall Schreckensmeldungen haben**. Sie wandte aber ein, solange sich aufgrund solcher Nachrichte **keine Verhaltensänderung** feststellen lasse, sei deren Wirkung vernachlässigbar. Weiter bezweifelte sie, dass die Menschen aufgrund eines Vertrauensverlusts, tatsächlich weniger kommunizieren und weniger IT benützen würden. **Hernâni Marques** wandte jedoch ein, eine Studie der Universität Zürich zeige, dass sich die Menschen in den **sozialen Medien selbst zensieren** würden. Auch in der Schweiz seien nur wenige tausend Leute aktiv auf Twitter. **Jürg Bühler** betonte, er halte als Stimmbürger die zunehmende **Diskrepanz zwischen Meinungsumfragen und Wahlergebnissen** für interessant. Die politische Landschaft werde sich Gedanken machen müssen, woher das komme. **Dr. Ladina Caduff** meinte schliesslich, mit Blick auf die vielen **UN-Organisationen in der Schweiz** könne sie sich nicht vorstellen, dass wir für Hacker nicht hochinteressant wären.

Wie können wir als Gesellschaft mit Fake News umgehen?

Abschliessend widmete sich die Panel-Diskussion der Frage nach Lösungsstrategien. Ein möglicher Ansatz seien **Schulungsprogramme**, wie diese auch Microsoft durchführe, erläuterte **Dr. Ladina Caduff. Dr. Myriam Dunn-Cavelty** betonte erneut, **Polemik werde in Demokratien gebraucht**. Die automatisierte Erkennung von Fake News durch Maschinen halte sie für höchst gefährlich. Im Bereich Cybersicherheit kritisierte sie jedoch die teils zu **niedrigen Standards in Unternehmen**. Man müsse auch über die Bestrafung von Firmen diskutieren, wenn diese beispielsweise in fahrlässiger Weise massenhaft Kundendaten verlieren. **Anne-Marie Buzatu** schlug den Bogen zur Covid-19 Pandemie. Diese habe uns bewusst gemacht, dass **verlässliche Informationen essenziell sind.** Sie erachte insbesondere **Kampagnen für Medienkompetenz** als bedeutende Massnahme von Regierungen gegen die Verbreitung von Fake News. Aufgrund der hohen Bedeutung der Wirtschaft sei der Einfluss von Regierungen jedoch beschränkt. Es brauche die **Zusammenarbeit verschiedener Akteure**.

Anschliessend wurde die Paneldiskussion für das Publikum geöffnet. Dominik Knill, Präsident der KOG Thurgau, fragte nach der Bedeutung von Gerüchten, diese seien quasi die **Urform von Fake News**. Die Forschung zeige, dass Gerüchte in gewissen Fällen tatsächlich Kriege auslösen können, antwortete **Dr. Myriam Dunn-Cavelty**. Allerdings stelle sich die Frage nach Ursache und Wirkung, denn bereits destabilisierte Gesellschaften seien anfälliger für Gerüchte. Zudem seien Gesellschaften, in denen **«Circuit Breaker»** vorhanden sind, weniger gefährdet. **Hernâni Marques** brachte das Beispiel von Taiwan ein, welches ein Digitalministerium betreibt. Dieses reagiere regelmässig mit **Fakten** auf Fehlinformationen aus der Volksrepublik China, im Sinne einer gezielten **«Gegenpropaganda»**, um die taiwanesische Bevölkerung sofort zu informieren.

Peter Beschnidt, zweiter Verteidigungsattaché von Deutschland in der Schweiz, stellte ernüchternd fest, dass **Schweizer KMUs wenig in Cybersecurity investieren**. Gefragt nach den Ratschlägen von Microsoft, antwortete **Dr. Ladina Caduff**, dass es aus ihrer Sicht ebenfalls

noch **grosses Verbesserungspotenzial** gebe. Sie führe dies auf eine Mischung aus **Kosteneinsparungen** und mangelnden **Geschäftsmodell-Innovationen** zurück. Es brauche aber auch eine **Bewegung in den Köpfen**, externe Hilfe im Bereich Cybersecurity zu akzeptieren. Darauf aufbauend warf **Hernâni Marques** die Frage auf, ob man angesichts der kürzlich identifizierten Sicherheitslücken bei Stimmenzählsystemen nicht **Mindeststandards für IT-Sicherheit** bei bestimmten kritischen Infrastrukturen einführen wolle.

Diesen Punkt nahm **Tomohiro Bisang,** Student an der Universität St. Gallen, auf: Wenn man **kritische Infrastrukturen vom Internet abkoppeln wolle**, wie vorgeschlagen, welche sollten das sein? Aus seiner Sicht, so **Hernâni Marques**, sollten **Wahlsysteme** ohne Internetzugang sein. In anderen Bereichen müssen man überlegen, wie man digitalisiert, beispielsweise beim **elektronische Patientendossier**. Man sollte auch **Lehren für kritische Infrastrukturen aus der Covid-19 Krise** ziehen, fügte **Dr. Ladina Caduff** an. Diese habe gezeigt, welche Systeme integral sind und abgekoppelt werden sollten.

Eigenverantwortung, Medienkompetenz und keine Überreaktionen!

In seinem Schlussstatement betonte **Jürg Bühler**, man solle sich im Umgang mit Fake News nicht von Emotionen leiten lassen, sondern immer wieder hinterfragen, was plausibel ist: «**Laugh with your heart, for everything else use your brain**». **Anne-Marie Buzatu** stimmte zu, dass wir alle einen **Reflex** haben sollten, selbst **Informationen** zu **verifizieren**. **Dr. Ladina Caduff** betonte, wir bräuchten erstens eine **minimale Beurteilungsfähigkeit der Technologie**, um zu entscheiden, was richtig ist. Zweitens gelte es, in der digitalen Welt, einen **möglichst nachhaltigen Raum** zu schaffen. **Dr. Myriam Dunn-Cavelty** forderte, das Internet nicht mit Regulierungen zu erdrücken. Eine Demokratie **brauche keine Instanz**, welche ihr sagt, was **fake oder nicht fake** ist. **Hernâni Marques** betonte ebenfalls die zentrale Rolle von **Medienkompetenz**. Weiter brauche es transparente Soft- und Hardware, eine Dezentralisierung der Systeme, Verschlüsselung zum Schutz gegen Überwachung und schliesslich ein **Bekenntnis zu einer freiheitlich-demokratischen Grundordnung**.

In seinem Schlusswort betonte **Silvan Künzle**, Präsident des Sicherheitspolitischen Forums St. Gallen, es sei das Anliegen gewesen, Studenten und Experten im Rahmen der Kooperation mit dem FORUM SICHERHEIT SCHWEIZ zusammenzubringen. Er stellte erfreut fest, dass dies gelungen sei und die heutige Veranstaltung sehr viele wichtige Fakten und Erkenntnisse zu Tage gefördert habe: **Fake News gab es schon immer** und das werde so bleiben. Die Welt sei aber kleiner geworden und Informationen verbreiten sich immer schneller. Es gelte daher **Resilienz aufzubauen** und **Medienkompetenz zu schärfen**, um den **Informationsüberfluss** richtig einschätzen zu können.