Fake News and Digital Safety

Concluding Raport| 7. SSF Security Talk of October 1, 2020, University of St. Gallen

Misleading newspaper articles, false reports on the internet, disinformation campaigns on social media, fake-news attacks on individuals, companies, organizations, governments, and countries pose a serious threat to open societies and democracies. The speakers at the 7th SSF Security Talk urged not to overreact but to tackle the problem with self-responsibility and media literacy.

Around 100 decision-makers, students and interested guests attended the 7th SSF Security Talk at the University of St. Gallen which was organized by the SWISS SECURITY FORUM in cooperation with the St. Gallen Forum on Security Policy. **Mayor Thomas Scheitlin** welcomed the speakers and guests at the beginning of the event. The citizens of St. Gallen are very proud of the University of St. Gallen, he stressed, as it is a key success factor for **education and research in St. Gallen.** Another success factor is the IT-cluster «IT St. Gallen Rockt» which brings together 90 enterprises, 16 education partners and 35 network partners, as well as the planned innovation park in the western part of the city. «Fake News or not?» - No, Scheitlin said, his statements are true and could be checked. Real fake news however affect the men and women in the streets when media and politics suffer from a loss in credibility. However, Scheitlin remarked, **fake news is not a new phenomenon**, but the ways and the speed of their distribution have changed.

A global buffet of misinformation

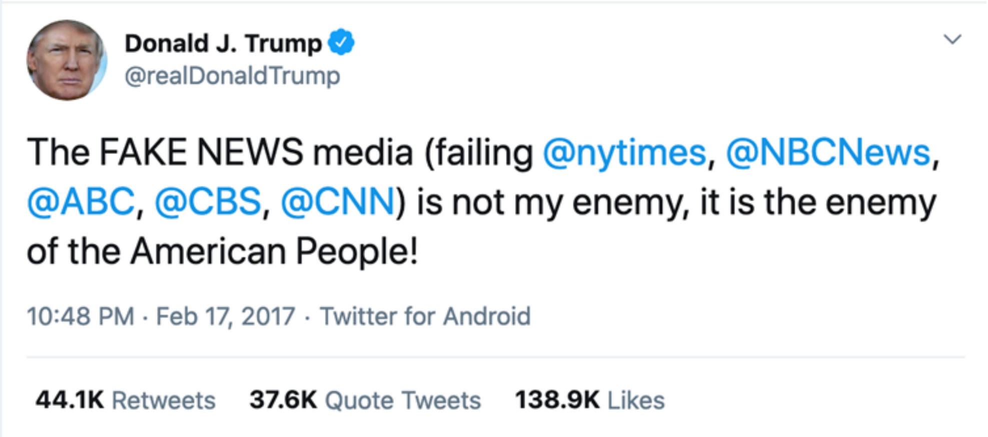
In the first keynote speech, **Jürg Bühler**, vice-director of the Federal Intelligence Service (FIS), explained the activities of the FIS in relation to fake news and **influencing operations**. Bühler stressed that the FIS is only responsible for a part of the problem – **influencing operations** by foreign governmental actors which are directed at the functioning of Switzerland and its society. In Switzerland, the FIS does not deal with those phenomena except if there are clear signs that a foreign intelligence service is active in Switzerland. Misinformation is **not a new phenomenon**, Jürg Bühler stressed as well. The **information space** has been **a part of conflicts** for a long time. But to know what information is true, remains essential for the autonomous decision-making of Switzerland and is, therefore, a key concern for the FIS.

The effect of influencing operations can hardly be measured especially because the reaction of the target groups cannot easily be measured. Many influencing operations do not want to spread a specific narrative but **cause as much confusion as possible** so that the **truth is lost**. Bühler said, this method had been applied after the assassination attempt of the former russian spy **Sergej Skripal** as well as after the poisoning of the oppositionist **Alexei Nawalny**.

However, the FIS has so far not found **any signs for the influencing of elections in Switzerland**. Bühler supposed Switzerland was probably not important enough internationally but, at the same time, the decentral organisation and the multi-party system of Switzerland would contribute to its protection. Bühler further explained the digitalization would increase the spread of fake news: «What once had been the *Stammtisch* has now become a **global buffet** from which everyone can take a piece but to which everyone can add something as well». Therefore, we would need to keep this phenomenon down as a whole society.

The truth as such does not exist

Dr. Myriam Dunn-Cavelty, senior lecturer for security studies and deputy for research and teaching at the Center for Security Studies (CSS), stressed in the second keynote speech that we would need to distinguish between **two meanings of «fake news»**. On the one hand, «fake news» means **targeted, distorted false messages** which can be identified through fact checking. On the other hand, the term «fake news» is being used, freely adapted from Donald Trump, to discredit the media. This kind of fake news originates from the **interplay between different truths,** especially when people prefer to trust their feelings than facts in times of post-factual tendencies.



Donald J. Trump
@realDonaldTrump

The FAKE NEWS media (failing @nytimes, @NBCNews, @ABC, @CBS, @CNN) is not my enemy, it is the enemy of the American People!

10:48 PM · Feb 17, 2017 · Twitter for Android

44.1K Retweets **37.6K** Quote Tweets **138.9K** Likes

Quelle: Präsentation Dr. Myriam Dunn-Cavelty

Dr. Myriam Dunn-Cavelty also stressed that **targeted misinformation** was **nothing new**. **Different truths** have always existed in society and that, she said, was a good thing. The political exploitation of the knowledge about their existence is nothing new but over time these tendencies have become subcultures. Today, these subcultures become more present again and conspiracy theories are increasingly instrumentalized politically. Dr. Myriam Dunn-Cavelty explained **technology was not the cause of this phenomenon,** but probably a booster. We no longer experience many important things on our own and thus in a comprehensible way but only through «the media». Because we increasingly consume foreign, especially American, media, a one-sided **global awareness for problems** has been created. At the same time, the media landscape has been drastically reduced. Today, there is lack of **«circuit breakers»**, journalists who go in-depth and can potentially identify fake news and stop their spread. Instead, **algorithms** are being used which speed up the spread of fake news.

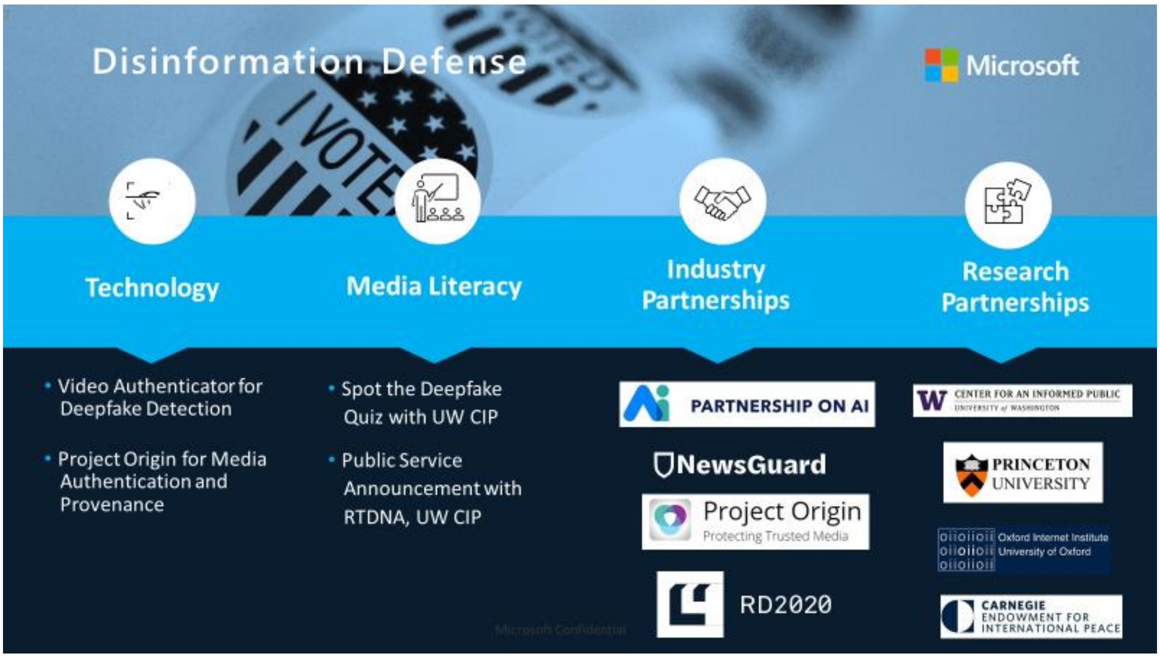
However, the **problem in Switzerland is very small**, Dr. Myriam Dunn-Cavelty said. As a society, we should therefore not overreact. This would only contribute to the destabilizing goals of fake news. One reason for our potential overreaction is that we always **overestimate the role of technology**. Fake news should therefore go beyond the theoretical debate. We need studies on whether there really is an effect of fake news in Switzerland. However, research on these issues is only beginning. To conclude, Dr. Myriam Dunn-Cavelty again stressed that **the truth as such does not exist**. Therefore, **no entity can define the truth**. Instead she urged society to build up **resilience**, the capability to withstand threats, in the face of the existence of different truths.

Shared responsibility for the development of a sustainable cyberspace

What responsibility do market and state bear for fake news and digital safety? – This was the topic of the third keynote speech by **Dr. Ladina Caduff**, Director Corporate Affairs at Microsoft Switzerland. In the beginning, Dr. Ladina Caduff stressed that the **world was more connected than ever before**. Until 2030, it is expected there will be 50 billion connected devices and already today 15 – 25% of global GDP is generated by the data economy. In order to use new technologies to create value **media literacy** and **tech capability** are needed, i.e. the ability by each individual to judge, but also, of the government, what technologies can and cannot do.

The decisive factor for the successful adaptation of new technologies is, however, **trust** – in products, in providers and in the cyberspace.

With regards to the threat situation, Dr. Ladina Caduff stated, there is a shift from cyber criminality to **cyber warfare**. The scale, the sophistication and the scope of the effects of cyber-attacks motivated by nation states have clearly increased. However, compared to conventional warfare, there are important differences. The cyberspace eludes the control of national and international jurisdiction. There is no **«digital» Geneva Convention** to protect citizens during military conflict. On the other hand, the cyberspace is primarily run and protected by private companies. Tech-companies such as Microsoft, therefore, are the **first responders to cyber-attacks.**



Disinformation Defense

Microsoft

Technology

- Video Authenticator for Deepfake Detection
- Project Origin for Media Authentication and Provenance

Media Literacy

- Spot the Deepfake Quiz with UW CIP
- Public Service Announcement with RTDNA, UW CIP

Industry Partnerships

PARTNERSHIP ON AI
NewsGuard
Project Origin Protecting Trusted Media
RD2020

Research Partnerships

CENTER FOR AN INFORMED PUBLIC UNIVERSITY of WASHINGTON
PRINCETON UNIVERSITY
Oxford Internet Institute University of Oxford
CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

Microsoft Confidential

Quelle: Präsentation Dr. Ladina Caduff

Out of awareness for this role, Microsoft has launched its **Defending Democracy Program** which is based on three pillars: Election Integrity, Campaign Security and **Disinformation**. To deal with misinformation, Dr. Ladina Caduff stated, there are, on the one hand, technological means, e.g. tools to recognize deep fakes. On the other hand, **media literacy** is needed which is why Microsoft educates individuals and political parties in dealing with information. However, there is only so much Microsoft can do without partnerships with other companies. One example is the **Cybersecurity Tech Accord**, in which more than 30 international companies undertake to invest in cyber security. To tackle the problem of normalizing the cyberspace, however, **multi-stakeholder dialogues** like the **Paris Call for Trust and Security in Cyberspace** are needed which bring together companies, states and civil society. Because it is in the interest of all of us, Dr. Ladina Caduff stressed in her conclusion, to make the **cyberspace as stable as possible** and **sustainable for future generations.**

Making the digital world transparent

After the keynote speeches, the audience saw a **video message** by **Vera Jourova**, Vice-President of the European Commission for Values and Transparency. Vera Jourova stated the Covid-19 crisis had shown how much we rely on technology. Therefore, we need to make the right decisions today to ensure that technology continues to serve us in the future because technology also creates risks for our safety and our democracy. This has been shown by the **«Infodemic»** during the Covid-19 pandemic, that is the overflow of information about the virus. The problem is exacerbated by domestic and foreign actors who abuse technology as weapons. For the European Commission, the time has therefore come to act and to **make the digital world more transparent**. The **Digital Services Act** is supposed to force platforms to act responsibly, especially with regards to illegal content, and to prevent a fragmentation of the digital common market. At the same time, the Commission is working on solutions to make the **cyberspace more transparent** and to **increase cyber security in the Union**, Jourova said.

Fake News and digital security – how big is the problem?

For the panel discussion, the **moderator Fredy Müller**, Managing Director of the SWISS SECURITY FORUM, welcomed in addition to the keynote speakers **Anne-Marie Buzatu**, Senior Advisor for the ICT4Peace Foundation, and **Hernâni Marques**, member of the board of the Chaos Computer Switzerland. Asked about her assessment of the initiatives by the European Commission, **Anne-Marie Buzatu** said, they were the **start of a conversation** about the normalization of cyberspace. Transparency and knowledge about where sources come from in cyberspace, were essential, she added.

Jürg Bühler ascertained that the intensity of cyber-attacks and misinformation has **increased in the last years,** even though attacks by state actors in cyberspace are nothing new. In his opinion, this is, however, a surrogate of rising international tensions. From a scientific perspective, it is very difficult to determine the **effect of fake news**, **Dr. Myriam Dunn-Cavelty** said. The Center for Security Studies has launched a project in Ukraine where they want to monitor fake news live during the coming elections. Afterwards, study participants will be asked in panel discussions if and which factors made a difference for them.

Hernâni Marques criticized the practice of international tech companies to **collect massive amounts of data**. There is so much data available about us today, he explained, that each of us can be approached with targeted information. In his opinion, these companies must be tamed. **Dr. Ladina Caduff** answered Microsoft was dealing very carefully with the question of **monopoly position in platform issues.** Other than Facebook and Twitter, Microsoft is, however, a data processor. Dr. Ladina Caduff furthermore stressed that **data security and protection of privacy** are a **shared responsibility**. Microsoft does a lot to make its products safer, but the customers must bear a part of the responsibility as well. From the perspective of Microsoft, **trust is essential** otherwise customers would not use technology anymore.

Podium
Moderation: Fredy Müller, Geschäftsführer FORUM SICHERHEIT SCHWEIZ
FORUM SICHERHEIT SCHWEIZ
Sicherheit geht uns alle an!
spf

The consequences of cyber-attacks on critical infrastructure

Wannacry showed the potential consequences of a cyber-attack on critical infrastructures. In British hospitals, **around 90'000 operations had to be postponed** because the computers of the hospitals were hacked. **Hernâni Marques** explained that Wannacry was caused by a security breach which had been developed by the NSA but later leaked to the public. Microsoft knew about the safety breach but kept it a secret. Hernâni Marques criticized the **hoarding of security breaches** by intelligence services as it would **undermine trust in IT-systems**. He demanded, Europe had to develop its own transparent IT-systems. **Dr. Myriam Dunn-Cavelty** added, the Internet had never been built for high security processes. The problem that state actors know about dangerous vulnerabilities of IT-systems, but do not disclose that information to the public, could not easily be solved. **Dr. Ladina Caduff** stressed, there is a need for **resilience** as well as that there is no **zero-risk society**. Microsoft, therefore, always tells its customers: «Assume breach!».

An attack like Wannacry would be **breaking a taboo** in the interstate arena, **Jürg Bühler** said. Unfortunately, such instruments are also available to private actors. Jürg Bühler personally believes, he said, that if **software producers** were subject to **equally strong legal liabilities** as it is custom for other products, their products would probably be less innovative but more secure. **Hernâni Marques** supported the statement that introducing liabilities would certainly be part of the solution. Especially with regards to autonomous vehicles, the manipulation of products could have fatal consequences. Products, therefore, need to be made so safe that **hacking them is no longer worth it**.

Hernâni Marques furthermore criticized the **«digitization mania»**. There is no need for digitalisation everywhere, he said. Some systems, e.g. nuclear power plants, should be disconnected from the Internet. Otherwise, the Internet of Things would become a **«Internet of Terror»**. **Dr. Ladina Caduff** stressed that, in the end, societies need to argue and decide how they want to use technology. Microsoft, however, has also registered in its **Cyber Defense Report**, which has been recently published for the first time, that **attacks on Internet-of-Things devices** have **increased by more than 35%** in the last year. ICT4Peace is trying as well to recognize new challenges such as autonomous driving way ahead of the rest of the international community, **Anne-Marie Buzatu** explained. She urged to **think about solutions before accidents happen**.

Fake News in Switzerland: hype or reality?

Afterwards, Fredy Müller directed the panellists' attention on the response to fake news phenomena in Switzerland. Because of the consumption of U.S. media, we are forced to balance American and Swiss news. **Dr. Myriam Dunn-Cavelty** took up this point from her keynote speech: It is part of modern societies that **there is disturbing news everywhere**. However, if this kind of news does not **cause a change in behaviour of the people**, their effect is negligible. Moreover, she shed some doubt on the assumption that people will communicate less and use less IT due to a loss of trust. **Hernâni Marques** responded, however, a study by the University of Zurich shows that people are **censoring themselves on social media**. Also, in Switzerland, only a few thousand people are active on Twitter. **Jürg Bühler** stated, as a citizen, he considers the increasing **discrepancy between opinion polls and voting results** highly interesting. The political landscape, in his opinion, will need to think about where this is coming from. **Dr. Ladina Caduff** finally said with regards to the many **UN-organizations located in Switzerland,** she could not imagine that we were not highly interesting for hackers.

How can we deal with fake news as a society?

Finally, the panel discussion focussed on the issue of solutions. One possible way are **educational programs** such as those offered by Microsoft, **Dr. Ladina Caduff** explained. **Dr. Myriam Dunn-Cavelty** stressed again **democracies need polemics**. In her opinion, the automated recognition of fake news by machines is highly dangerous. With regards to cyber security, on the other hand, she criticized the **standards for companies were sometimes too low**. We should also discuss the punishment of companies if they negligently lose mass amounts of customer data. **Anne-Marie Buzatu** made the connection to the Covid-19 pandemic. The pandemic has shown us that **reliable information is essential**. Therefore, she especially considered **media literacy campaigns** as significant governmental measures against the spread of fake news. Because of the high importance of businesses, the influence of governments is restricted however, she added. Therefore, the **different actors need to work together**.

After this statement, **the panel discussion was opened to the audience**. **Dominik Knill,** President of the KOG Thurgau, asked about the importance of rumours which are, in some sense, the **original form of fake news**. **Dr. Myriam Dunn-Cavelty** answered that research has shown that rumours can in some cases cause wars. However, the question is whether they are the cause or effect of wars. Namely because societies that have already been destabilized and are more vulnerable to rumours. On the other hand, societies in which there are **«circuit breakers»** are less at risk. **Hernâni Marques** added the example of Taiwan which has a digital ministry. This digital ministry regularly reacts with **facts** on misinformation from the People's Republic of China in the sense of a targeted **«counter-propaganda»** to inform the Taiwanese population directly.

Peter Beschnidt, second defense attaché of Germany in Switzerland, determined with disillusion that **Swiss SMEs invest too little in cyber security.** Asked about the advice of Microsoft, **Dr. Ladina Caduff** agreed that there is **a lot of room for improvement**. In her opinion, this is due to both **cost saving measures** and a lack of **business model innovation**. However, there also needs to be **a change of mindset** to accept external help in cyber security. **Hernâni Marques** added the question whether we would need to introduce **minimum standards for IT-security** in certain critical infrastructures, especially with regards to the recently detected security gaps in vote counting systems.

Tomohiro Bisang, student at the University of St. Gallen, took up this point: If we want to **cut off critical infrastructures form the Internet,** as has been proposed, which ones should they be? In his opinion, **Hernâni Marques** said, **voting systems** should not have access to the

Internet. In other areas, we should think about if and how we want to digitalise, e.g. the **electronic health record**. **Dr. Ladina Caduff** added we should also **draw lessons about critical infrastructures from the Covid-19 crisis**. The crisis has shown, which systems are integral and should be cut off from the Internet.

Self-responsibility, media literacy and no overreaction!

In his closing statement, **Jürg Bühler** stressed in dealing with fake news, we should not let ourselves be guided by our emotions but continuously reflect what information is plausible: «**Laugh with your heart, for everything else use your brain**». **Anne-Marie Buzatu** agreed that we should all have a **reflex to verify information** by ourselves. **Dr. Ladina Caduff** stressed tjat firstly we need a **minimum ability to evaluate technology** to decide what is right. Secondly, we need to create a **cyberspace** that is **as sustainable as possible**. **Dr. Myriam Dunn-Cavelty** urged not to suffocate the Internet with regulation. A democracy has **no need for an entity** to tell it **what is fake and what is not fake. Hernâni Marques** also stressed the central role of **medial literacy**. Furthermore, we need transparent soft- and hardware, a decentralisation of systems, encryption to protect against surveillance and, finally, an **acknowledgement of our liberal-democratic order**, he added.

In his closing word, **Silvan Künzle**, President of the St. Gallen Forum on Security Policy, stressed it had been their desire to bring students and experts together through the cooperation with the SWISS SECURITY FORUM. He was pleased to note that this was achieved, and that today's event had brought to light many important facts and insights: **Fake news have always existed** and will continue to exist. The world has, however, become a smaller place and information spreads faster and faster. Therefore, it is required to **build up resilience** and to **boost media literacy** to be able to cope with the **overflow of information.**

We thank our sponsors!

helvetia
Ihre Schweizer Versicherung

spf
Sicherheitspolitisches Forum
St.Gallen

ICTSWITZERLAND
UMBRELLA ORGANISATION FOR THE DIGITAL ECONOMY

Media Partner:

TAGBLATT