satw

Information Warfare

Cybersecurity – challenges for political Switzerland

State of the art

Information warfare is a growing threat, particularly for western democracies, to which all social players are exposed. In this section, we identify the measures that state players in particular need to take to determine their role and responsibilities and to highlight priority areas of action.

The issue of information warfare has a long tradition, both internationally and in Switzerland. In the late 1990s to around 2010, the umbrella term covered all relevant issues, including warfare in cyberspace, propaganda, disinformation and psychological warfare. The issue was addressed both as part of the Strategic Management Exercise 97 (SFÜ) and conceptually within the Swiss Army as part of the Information Operations Conception Study (KS IO). The current use of the term increasingly refers to the influencing of public opinion using semantic methods in which technological aspects are one of the driving forces for the implementation of these operations.

In the 1990s, various organisations and researchers raised awareness of possible developments relating to the use of digital technology for the production and dissemination of information manipulated in various ways. However, this only became relevant and real with the emergence of social media and the wider availability of machine/deep learning technologies at affordable prices.

The use of artificial intelligence algorithms, automation, and large data volumes on the web and in social media is changing the scope, range and precision of how computer-based propaganda campaigns can be used to manipulate public opinion. Today it is possible to produce content automatically or semi-automatically, to convert it into text, language and images and to make it available to a broad and target-group-specific mass of people in a short space of time and without significant costs. The nature of social media makes it highly susceptible to attacks.

Recommendations

1. Development of state capabilities to detect and attribute influencing operations. This should involve all levels of the state (Federal Government, cantons, municipalities) and be coordinated at Federal Government level.
2. Checking legal basis to enable responses to influencing operations and establishing clear guidelines for possible defensive options or counter-attacks.
3. Cooperation with the national media to expose disinformation and to raise public awareness of the issue.
4. Making agreements with major social platforms which can be used in Switzerland to support the combating of social media influencing operations.
5. Creation of an alarm system for ongoing attacks (such as SwissAlert or as part of it).
6. Political coordination with the European Union on combating social media influencing operations, e.g. in tandem with social media platforms.
7. Incorporation of social media expertise and awareness of digital risks into education programmes.
8. Support of fact-checking initiatives specially aimed at the Swiss context.

Filter bubbles and echo chambers can be created and enhanced; memes, photos and videos can be used for the dissemination of information without the ability to verify the source; communities can be attacked by identifying vulnerable personal profiles or influential network nodes.

Social media is being manipulated by governments and political parties. According to a study by the Oxford Internet Institute[1], there is evidence of organised social media manipulation campaigns by cyber-armies or political parties for 70 countries in 2019 compared to 48 countries in 2018 and 28 in 2017. In authoritarian states, social media manipulation is used as an instrument to control the population. Democratic states are the target of influencing operations which are carried out by a handful of players, including (according to the evidence) China, India, Iran, Pakistan, Russia, Saudi Arabia and Venezuela. The size of the cyber-army in China is currently estimated at 300,000 to 2 million people. Cyber-armies often also work with the private sector, civil society organisations, internet subcultures, youth groups, hacker groups, fringe movements, social media influencers and volunteers who support their cause ideologically.

A wide range of techniques are available for implementing influencing campaigns, including disinformation, social hacking, fraudulent identities, bots and trolling. One thing all these techniques have in common is that they are used to influence political processes (e.g. elections) or even spark uprisings and revolutions. The destabilising potential of this type of warfare is based on a deeper understanding of human decision-making processes and the dynamics of mass phenomena. These aspects can also be simulated increasingly easily thanks to new technology and algorithms.

Challenges

Operations that attempt to influence at the state level can change public opinion in a country in favour of the attacker. This means that democracies where political decision-making processes are firmly embedded in public opinion are particularly susceptible to this kind of attack.

Influencing operations are attractive to attackers for various reasons:

1. They are relatively inexpensive to carry out
2. They are difficult to attribute and the risk of escalation is limited
3. They enable the instrumentalisation of users on a large scale
4. They can be used alone or in combination with other forms of warfare (traditional, economic).

On the other hand, it is difficult to determine the efficiency and impact of influencing operations. They also run the risk of slipping out of control for attackers. It can nonetheless be assumed that changes in public opinion were achieved in several recent events, in particular the elections in the USA, UK and France. The question remains as to whether these changes ultimately proved decisive.

Another unanswered question is whether Switzerland has already been the target of sophisticated influencing operations. There are indications that they have taken place on certain political issues (e.g. referendum on Billag, 5G controversy).

Need for action

The position of the Swiss government is that the active use of manipulated information to achieve political objectives is not an appropriate tool for a democratic state. This is why it is extremely important that the following measures are implemented in response to the threat from information warfare (also see the EU Action Plan):

1. **Capabilities for the identification, analysis and attribution of influencing operations:** Actions by third parties in a state's own sphere of interest must be **identified**, **analysed** and **attributed** at an early stage. Access to relevant data and data analysis tools as well as human analytical capabilities are essential in this regard. They should form part of the capabilities of

the **state authorities** in collaboration with private players and based on international cooperation. The constant analysis of the semantic and technological approaches used helps to set up and ensure an effective early warning system. The aspect of time should not be overlooked: once distributed, false information can circulate for a long time undetected in the background and suddenly cause, for example, violent actions by a large number of people.

2. **Reaction to detected influencing operations**: As soon as they are detected, reactions by state authorities are implemented in line with the existing **legal basis**. Reactions may require warning systems, fact-based communication in the media or a limitation of the attacker's capacities. The state's own population should also be provided with access to reliable information and facts. This process must remain transparent and traceable so that the information distributed can be verified independently.

3. **Interaction between state authorities and the private sector**: To detect or respond to social manipulation, state actors are reliant on cooperation with the private sector, particularly with the operators of social media platforms and the media. In very serious cases, this cooperation can mean providing access to relevant data, closing suspected accounts, removing false information, or providing the public with information about such attacks and correcting disinformation.

4. **Increase in social resilience**: As social manipulation is targeted at the general public, raising society's awareness of this phenomenon is vitally important. Specific measures include educating people of all age groups about how to recognise and react to such attacks and involving the general population in defensive activities, such as fact-checking.

Basic rights, such as freedom of expression, are generally regarded as fundamental to our society and are firmly established in it – this means restrictions on access to information are only justified as a last resort in very serious cases of a criminal nature. This is why a prompt response in the form of information is also extremely important here.

References

– Action Plan Against Disinformation, Joint Communication to The European Parliament, The European Council, The Council, The European Economic and Social Committee and The Committee of The Regions, Brussels, 5.12.2018 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019JC0012

– Cyber Influence Operations: An Overview and Comparative Analysis, Center for Security Studies (CSS), ETH Zurich, Zurich, October 2019 https://css.ethz.ch/en/services/digital-library/publications/publication.html/c4ec0cea-62d0-4d1d-aed2-5f6103d89f93

– The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation. Working Paper Oxford, 2.2019 https://comprop.oii.ox.ac.uk/research/cybertroops2019/

Appendix

Explanation of some common forms of information warfare

– **Disinformation**: Distributing false or incomplete information with the intention of deception.

– **Social hacking**: Use of socio-cognitive characteristics of the human mind, particularly tribalism and tendency to conform.

Fraudulent identities: Use of legitimate identities by illegitimate actors.

– **Bots**: Automated computer software for the manipulation of online platforms.

– **Trolls**: Users or bots that attack or insult other users in a targeted way.

Contact

Nicole Wettstein
Head of priority programme Cybersecurity
+41 44 226 50 13

https://www.satw.ch/cybersecurity-challenges

Impressum
Swiss Academy of Engineering Sciences SATW
Expert contributions
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Board of Directors and Advisor | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Editing and graphics
Beatrice Huber, Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
September 2020