Bundesministerium
des Innern
und für Heimat

Increasing awareness in dealing with hybrid threats, including disinformation

Recommendations of the Open Joint Federal and State Working Group on Hybrid Threats (BLoAG Hybrid) to increase awareness in dealing with hybrid threats, including disinformation

For distribution to federal state ministries and local governments

The term "hybrid threats" refers to various forms of illegitimate influence by foreign governments. These foreign governments coordinate and use different instruments, including non-state actors, to try to achieve their objectives, openly or covertly, in opposition to our interests and values. In the process, they seek to weaken and destabilise our democracy. The instruments they use include for example disinformation; cyber attacks on government bodies and on businesses and industry; espionage and industrial espionage; theft of intellectual property; economic influence, for example through investment in key industries; sabotage of critical infrastructure; and interference with free elections. In terms of security policy, disinformation that is directly or indirectly controlled by foreign states is categorised as a hybrid threat.[1] It should be noted, however, that disinformation is also deliberately used and disseminated by actors within Germany to destabilise our government and society.

Hybrid threats affect all levels of government and society. They may involve a combination of instruments to create a coordinated campaign. It is sometimes difficult to recognise individual incidents as part of a larger campaign and to respond in time.

A well-known example of disinformation with the potential to divide society is the 2016 incident ("Fall Lisa") involving a 13-year-old ethnic Russian girl in Berlin who claimed that she had been kidnapped and raped by three refugees.[2] Another example is a video, later found to be fake, that circulated in Russian-language social media in 2022 reporting that a 16-year-old boy in Euskirchen had been beaten to death by a gang of Ukrainians.[3] An example of foreign manipulation and interference in the information space is the "Doppelgänger" campaign to copy or "clone" the websites and social media accounts of legitimate Western media in order to disseminate disinformation.[4] Phishing attacks by the cyber actor "Ghostwriter" are an example of cyber attacks.[5] Associations, cultural institutes and city twinning programmes can also be exploited for use in foreign interference operations.[6] Earlier this year, a foreign operation was

[1] For a description of hybrid threats, including disinformation, see https://www.bmi.bund.de/DE/themen/heimat-integration/wehrhafte-demokratie/abwehr-hybrider-bedrohungen/abwehr-hybrider-bedrohungen-node.html.
[2] https://www.bpb.de/themen/migration-integration/russlanddeutsche/271945/der-fall-lisa/ https://www.sueddeutsche.de/panorama/urteil-in-berlin-fall-lisa-endet-mit-bewaehrung-1.3553054
[3] https://www.ruhrnachrichten.de/regionales/ukrainer-pruegeln-jugendlichen-in-nrw-zu-tode-polizei-warnt-vor-fake-video-w1737591-2000483586/. See also Mascolo, Georg, "Die neuen Waffen", *Süddeutsche Zeitung*, 10 June 2023)
[4] https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/2023/article/statement-by-ms-catherine-colonna-foreign-digital-interference-france-s https://euvsdisinfo.eu/de/eines-dieser-dinge-ist-nicht-wie-die-anderen/ Engl: https://www.disinfo.eu/doppelganger/
[5] https://www.spiegel.de/politik/deutschland/russischer-hack-erneute-attacke-hack-auf-bundestag-sieben-abgeordnete-betroffen-a-75e1adbe-4462-4e30-bd94-96796aed6b8a
[6] https://merics.org/de/studie/stadt-land-fluss-im-blick-beijings-chinas-subnationale-diplomatie-deutschland https://www.welt.de/politik/ausland/article235115984/Staedtepartnerschaften-Foederalismus-spielt-China-in-die-Haende.htmlhttps://www.faz.net/aktuell/politik/inland/china-die-strategie-hinter-den-staedtepartnerschaften-18832083.html

found to be spying on railway routes in Poland used to transport weapons to Ukraine.[7] Such a spying operation is conceivable in Germany too. The case of a Chinese scientist at Heidelberg University's Institute of Physics is an example of how intellectual property generated in Germany with German and European funding was taken to China for commercial and military uses.[8]

The greatest challenges are recognising and averting hybrid threats, coordinating the action necessary to do so, and making government and society more resilient to such threats. The following measures can help:

1. Sharing information

Inform your staff about hybrid threats, including disinformation. Identify units within your ministry or local government where foreign governments could exert influence and make sure that your staff are well-informed about the risks and the precise tools used. Designate a contact person or unit responsible for dealing with hybrid threats and regularly provide staff with the relevant training and information in different formats. Encourage your staff to seek out this contact person or unit if they have questions.

2. Public outreach

Within the scope of your ministry's or local government's responsibilities, intensify your proactive public outreach on this issue. Doing so can increase public support for measures to fight hybrid threats and disinformation.

3. Dealing with disinformation

Encourage communication between your public information staff and the relevant subject-related units, among other things to counteract false or misleading information. All of your communication should be proactive, transparent and fact-based. Respond without delay to false information that directly relates to your ministry or local government and publish a correction.

4. Protecting critical infrastructure

Identify relevant critical infrastructures in your area of responsibility. Contact the operators of these critical infrastructures regularly to discuss their operational risk analyses. Make the operators aware of the need for suitable resilience measures, based on their risk analyses, to keep their infrastructures operational. To maintain the provision of public services even in the event of attack, you can work with the operators of critical infrastructures in the framework of integrated risk management as outlined in DIN SPEC 91390:2019-12. The protection strategies and

[7] https://www.rnd.de/politik/polen-russischer-spionagering-soll-polnische-bahnstrecken-ausgespaeht-haben-versteckte-kameras-PQNYUEW5RS347HYZXI4D5JHYYE.html
[8] https://correctiv.org/aktuelles/china-science-investigation/2023/06/13/wie-die-uni-heidelberg-teil-von-chinas-quantenstrategie-wurde/
Engl: https://www.dw.com/en/chinas-quantum-leap-made-in-germany/a-65890662

recommendations published by the Federal Office of Civil Protection and Disaster Assistance (BBK) and the Federal Office for Information Security (BSI) should be followed.

5. Cyber security

Familiarise yourself with the specific requirements for IT security in your state or local administration and take advantage of the advisory services offered by your responsible IT security organisation. Provide sufficient security for your IT by making sure that all of your systems, data and networks are secure, by checking regularly for vulnerabilities and by closing any gaps in security. Use strong passwords, two-factor authentication and encryption to increase the security of your data. Include all terminal equipment used in the workplace and for telecommuting in a robust access management system. Increase awareness among your staff and designate persons to contact for more information.

6. Emergency planning

Develop emergency plans and crisis response strategies which are easily understood and compatible with other such plans and strategies which may already exist, in order to be able to respond to possible scenarios quickly and effectively. Test these plans and strategies regularly, if possible under realistic conditions, to make sure that they will work in a real emergency.

7. Economic and research security

Protecting businesses and research institutions against espionage and sabotage must be a priority for top-level management. Seek to maintain a climate of openness and a culture of error management, because contented employees are less likely to mount insider attacks. Conduct a risk analysis. Identify your tangible and intangible assets that require protection; consider which actors could be interested in them and in what ways these assets could be at risk of theft or manipulation, for example. Based on this assessment, develop measures to protect these assets. Classify relevant data by degree of confidentiality and determine who must have access to them. When starting new collaborations, carefully examine whom you will be working with in future. If possible, search for information in the language of your potential business or research partner. You can find more information about economic and research security on the website of the Federal Office for the Protection of the Constitution (BfV). [9]

8. Cooperation

Identify organisations, agencies, institutions and interest groups which are appropriate and necessary partners for cooperation. Create networks with the essential organisations and operational units and regularly discuss threats and how to deal with them together.

[9] Engl: https://www.verfassungsschutz.de/EN/topics/economic-and-scientific-protection/economic-and-scientific-protection_node.html

9. Initial and advanced training

Provide your staff regularly with current information as well as initial and advanced training on dealing with hybrid threats including disinformation. Identify organisational units in your ministry or local government which require more intensive advanced training. Encourage your staff to take media literacy courses regularly in order to keep up with the latest developments in new media and be able to recognise disinformation quickly.

10. Staff qualifications

Staff members, for example those working in the area of international relations, should have or should acquire the necessary qualifications, such as the relevant foreign language skills, social media skills or subject-specific training, and should be made aware of the specific risks related to working with the relevant countries.

11. Security-sensitive tasks of staff

Familiarise yourself with the regulations on personnel security and counter-sabotage, and contact the unit responsible for the security of classified information in your organisation if you have questions. Identify security-relevant organisational units and areas of activity (such as IT and records management). Conduct thorough background checks of new staff members before assigning them to work in sensitive areas. In addition to security vetting as part of personnel security and counter-sabotage, pre-employment screening in particular can assist with security-oriented hiring.

These recommendations are not exhaustive and should be adjusted depending on the sector, size and type of organisation. The measures should be checked regularly to ensure that they are up to date. The current contact information (email addresses, telephone numbers, etc.) of the responsible individuals/units should also be provided

Publication data

Published by:
Federal Ministry of the Interior and Community, 11014 Berlin, Germany
Website: www.bmi.bund.de

Last revised:
December 2023

Article number: BMI24024

You can also find further publications of the Federal Government to download or order at:
www.bundesregierung.de/publikationen