Metis

Study

Trends and developments in hybrid threats

No. 35 | June 2023

Institute for
Strategy & Foresight

Summary

Hybrid threats affect ever more areas of society. Hybrid actors exploit vulnerabilities of complex and highly networked societies in order to achieve political, ideological or economic objectives. This study examines new trends and developments in terms of hybrid threats and discusses future implications for national and international security.

Five generations of warfare

The first three generations of warfare were conventionally conducted conflicts between states. First-generation warfare (formation warfare) prevailed from antiquity to the 19th century and was characterised by line and column formations of uniformed heavy infantry. Second-generation warfare (firepower warfare) was dominated by greater accuracy and firepower of long-range weapons, rail transport and motorisation as well as increasing industrialisation of the war economy between 1850 and 1930. Increased firepower led to trench warfare and so the third generation of warfare (manoeuvre warfare) focused on combined arms operations based on tactics of speed and surprise. The aim was to bypass the enemy's lines and collapse their forces from the rear. The focus in the first three generations of warfare was on the physical destruction of enemy armed forces. Fourth-generation warfare (decentralised use of force) is aimed at undermining the psychological ability of an adversary to conduct warfare by using public pressure to force the hands of political decision-makers. Insurgents primarily use indirect warfare against the state to claim victims, especially in democratic states with a high level of casualty aversion. The civilian population, public opinion and decision-makers thus become the primary strategic focus. Fifth-generation warfare (non-kinetic military action) is dominated primarily by social engineering, the spreading of false information, cyber attacks, and the use of artificial intelligence (AI) and autonomous systems. Here, too, the aim is to influence the will of the public and their decision-makers by using non-kinetic means and technological innovations. All of these generations of warfare are ideal-type forms of war which are not mutually exclusive and may be applied simultaneously. States today thus face both conventional and hybrid threats which together constitute complex and dynamic security challenges.[1] The non-traditional means used in this context range from electoral influence and economic weakening to the planned dissemination of propaganda, cyber activities and espionage.

Cyber attacks that undermine infrastructure, financial systems or government institutions and disinformation campaigns that establish counter narratives are on the rise. Many hybrid threats also continue to entail the problem of attribution, which means that the initiators and perpetrators cannot be clearly identified, making it more difficult to hold them to account. What is more, attacks by state and non-state actors operating in a hybrid manner expand into other areas of society. In order to illustrate the transition from the fourth to the fifth and sixth generation, some current trends and developments in terms of new hybrid threats will be discussed in the following.

Current trends in disinformation

The spread of disinformation in order to disrupt social decision-making processes or to influence elections is nothing new. However, as a result of recent progress in the development of generative AI for texts and images, the quantity and quality of disinformation will improve. Chat bots on social media, for example, used to be relatively easy to spot because of the poor quality of their content and language and their repetitive lines of argument. AI-generated images

1 See "New hybrid threats", Metis Study No. 26 (July 2021).

could usually be identified even upon a cursory examination that involved looking for additional body parts, especially fingers. AI-generated videos and emulated voices of well-known public figures also did not require any forensic means to be identified as fake, for example, because of lip-sync errors and unnatural intonation. Since the release of generative AI models in late 2022, however, it has become possible to use only a few prompts to create realistic images, texts and videos that are difficult or impossible to identify as fake. Deepfakes generated by speech synthesis software and other technology turn the right to one's own picture into a relic of the past, thus influencing public debate and rendering data protection standards meaningless. Discussions on political and social issues between AI bots, together with elaborate comments, will appear to the average user like debates between experts and can thus influence public opinion.

Social media platforms as hybrid means

Social media platforms have become established as modern information and communication media and have reduced the market share of existing media formats. Disinformation accompanied their ascent from the very beginning. Government regulation as well as rules introduced by the operators themselves – depending on the different national contexts – use censorship, filters, community feedback, warnings and blocking of accounts in an effort to try and curb the spread of content that glorifies violence or is racist, sexist or obvious misinformation. Users, in turn, use less regulated messenger services such as Telegram in order to bypass these measures. US platforms such as Google (YouTube), Meta (Facebook, Instagram, WhatsApp) and Twitter primarily pursue economic interests and collect user data for advertising purposes.

Newly established video services such as TikTok, operated by the Chinese company ByteDance, represent an evolution of hybrid threats in the information area. They are no longer only battlefields of information – the platforms themselves are the hybrid means of exerting influence. The operator of TikTok has become the focus of worldwide criticism over concerns in connection with data protection and the protection of young persons as well as espionage and censorship for the benefit of the Chinese government. The company is not a mere private-sector operator committed to the maximisation of profit but a semi-governmental actor due to its proximity to the Chinese government. The app collects more data about users than similar applications. Officially, such data is used to improve algorithms. However, cyber experts have already proven in several cases that TikTok uses so-called back doors. In addition, the app conceals which data is collected and where it is sent. TikTok also has the capability to receive zipped files and to carry out executables. Malware, for example, could thus be transmitted undetected. When users select the highest privacy settings, the app leads them to believe that this configuration has been confirmed, yet the app will continue to send data in the background. The content on the app is mostly trivial, amusing and created by users themselves. Based on individual psychology, the algorithm, however, is optimised in such a way that its selection of short videos can draw in users for hours every day. Politically controversial issues such as videos on demonstrations in Hong Kong are purposely censored and replaced by trivial content. The algorithm creates a psychological profile of each user and slowly learns how to distract them or guide them towards a specific way of thinking by presenting specific content. Studies have proven that, especially among young users who consume TikTok for three to five hours a day, indifference to political, ethical and social issues, low productivity and a positive attitude toward China are increased. Thus, TikTok is a kind of Trojan horse that not only acts as a data leech and creates psychological profiles of all its users but is also used as a means of influencing them. The aim of TikTok seems to be to exert subliminal influence on an entire generation through trivialisation and distraction in order to manipulate future social decision-making processes. In China, TikTok is available under the name Douyin. Unlike in the rest of the world, this version of the app is a platform focused on education, technology and creative activities which tries to inspire its users to be more productive, creative and enterprising.

Churches and religious associations exerting hybrid influence

Churches and religious associations are increasingly used by external state and non-state actors to exert political influence. Domestically, the aim is primarily to promote the political, ideological or social positions of religious minorities, to influence voting behaviour and to establish legal concepts based on religious convictions. In most cases, the goal is to encourage social disintegration, to establish an authoritarian world view among followers and to spread religious ideas of society modelled after other states. In Germany, radical Christian, Islamic and cult-like communities have been known to spread anticonstitutional religious views through non-profit organisations for years. Vulnerable members of society are identified and targeted for recruitment in charity organisations and educational institutions. Critics within their own ranks are excluded under threat of violence while journalists who try to investigate risk being assaulted. An ever-increasing number of religious associations that use hybrid methods are directly or indirectly financed, supported and controlled by foreign state institutions. According to its statutes, the advisory committee of DITIB, the Turkish-Islamic Union of the Institute for Religion, for example, is obliged to appoint the President of the Directorate of Religious Affairs of the Republic of Turkey as its chairman. Since 2016, organisations such as the Kuwait-based Society of the Revival of Islamic Heritage, the Sheikh Eid Charitable Association from Qatar and the

Muslim World League based in Saudi Arabia have been known to finance mosques and facilities of Salafis in Europe.

At the international level, too, there is a trend towards religious institutions' being used to increase geopolitical power and control. When, for example, the Patriarch of Constantinople, the spiritual leader of the Orthodox Church, in 2018 granted autocephaly to the Orthodox Church of Ukraine, thus recognising its independence from the Russian-Orthodox church, Russia took this as an opportunity to proclaim a schism between Moscow and Constantinople. Since then, the Kremlin has increasingly exerted religious influence in predominantly orthodox states and has been trying to assume Constantinople's traditional leadership role. The open conflict between the Greek and the Russian Orthodox Church is thus not theological in nature but part of a hybrid campaign in the fight for religious leadership within the Orthodox Church. With the help of donors who are close to the Kremlin, Russia invests large amounts of money in the Monastic Community of Mount Athos in order to exert influence on the most important monasteries there. It has also tried to exert political and personnel influence to co-opt the Patriarchates of Alexandria, Antioch and Jerusalem in order to create majorities in the Ecumenical Patriarchate. Since 2018, more and more Russian clerics with a Turkish passport have been active in Turkey to ensure, with the help of the Turkish government, that the next Patriarch of Constantinople – or the one after – will be of Russian origin.[2] This would not only be the first Russian Orthodox patriarch in the 1,600-year history of the Patriarchate but also a political success for Russia on a global scale.

Sunni Saudi Arabia pursues similar aspirations of spiritual hegemony by spreading Wahhabism and Salafism, thus directly competing with Shiite Iran. Wahhabi ideas are promoted through the direct financial support of religious associations and educational institutions in Africa, Asia and Europe. In recent years, increased financial resources have been provided for this purpose and a multitude of new communication and dissemination methods have been experimented with in order to win over young, well-educated Muslims in particular. Previously, marginalised or ostracised individuals were the primary focus of information campaigns and recruitment efforts, often within religious institutions. The Salafist movement has spent enormous sums on social media as an instrument to reach students, young professionals, academics and other educated Muslims in recent years. Some Salafist channels on Facebook and YouTube have several million followers. It is likely that, if the monolithic view of Islam funded by Saudi Arabia becomes more widespread, the recruitment efforts of radical forces in local communities will continue to fall on fertile ground.

Autonomy and AI as weapons

Up to now, AI has been used mainly for data processing. By analysing large amounts of data and identifying patterns, AI can process military information faster and provide recommendations for tactical and strategic decisions. In a nutshell, this means that the ability to process more data in less time leads to quicker decisions and thus to victory. The Russo-Ukrainian war shows the increasing importance of processing power and the increased value of unmanned systems for warfare in the 21st century.[3] Commercial drones, for example, are used for reconnaissance and to share coordinates with artillery. Most of these systems are not autonomous; they still have to be controlled by operators who will decide whether and when to engage a target based on the images and video information transmitted in real-time. In short, humans are still the ones "pressing the button". Autonomy in weapon systems, on the other hand, refers to machines taking over functions that previously required human intervention, which has been controversially discussed, especially when it comes to target engagement. For decades now, weapon systems have been capable of autonomy with regard to the so-called critical functions. In fact, it has long been common practice for weapon systems to independently select and engage targets, especially to defend against incoming missiles such as rockets, artillery and mortar shells. In recent years, however, the range of functions of AI has increased enormously, especially in the field of object recognition, so that today machines are on the verge of assuming additional functions in ever more operational contexts, which gives rise to ethical, legal and security-related concerns.

Fuelled by Russian aggression and in view of the systemic confrontation between the US as the hegemon and China as its challenger, however, an AI arms race has already begun. In future wars, AI therefore will not only increase the capabilities and precision of kinetic weapons but will also appear in independently operating systems directed against societies away from the battlefields. AI will attack or control critical infrastructure, sensitive transportation, logistic and energy supply systems, the financial sector and administrative systems. AI will be employed in the cyber sector, both to attack and to defend critical systems. In the future, victory will thus become a matter of having the best AI. Countries that cannot keep pace with such an AI arms race will suffer setbacks in their political and economic importance as a result of their vulnerabilities and lack of

2 Due to the decreasing number of Orthodox Christians in Turkey, it will be difficult to elect a qualified head of the church. What is more, the training of priests in Turkey is currently prohibited by the state, but is considered a prerequisite. The only remaining Orthodox seminary was closed by the state in 1971, when all private universities were nationalised. It has not been reopened since. Theologians thus have to study abroad but risk being deprived of their Turkish citizenship.

3 See "Uncrewed systems: armaments, control and arms control", Metis Study No. 28 (June 2022).

resilience. Additionally, ongoing advances in the field of cognitive AI are associated with the risk of losing control. The emergence of a rogue AI[4] is therefore certain – it is just a matter of when.

Use of drones by non-state actors

The military use of commercial drones in the Russo-Ukrainian war also highlights the technological maturity of the systems currently available on the market. Non-state actors, too, are likely to take note. Mass attacks on military and state installations or spying activities by hybrid actors in barracks and defensive installations, which are already happening on occasion, will therefore become increasingly likely. The use of drones against critical infrastructure, to spy out security measures and for the reconnaissance of drug and smuggling routes is also plausible. In future, pirates will use drones to check whether container ships have armed security personnel on board and then decide whether an attack is worthwhile. Radical climate activists could use drones to spy out coal-fired power stations or oil refineries, to damage sensitive components or to set targeted fires. Terrorist drone attacks on aircraft taking off and landing would already be feasible today. As drones are likely going to become ever smaller and quieter, their identification, defence and tracking will become more difficult. In the future, it is likely that critical infrastructures can only be protected by extensive no-fly zones and jamming transmitters.

Implications of future hybrid threats – the sixth generation of warfare

As outlined above, new social fields of activity as well as emerging technologies dominate current developments of hybrid actions and influence. In the field of social media and disinformation, the platforms themselves are increasingly becoming the weapon, while AI-based processes improve the quality and credibility of false information. While Europe focuses on debating normative and legal control over AI as well as aspects of data protection, autocracies will use AI-based systems to undermine liberal democracies on a global level and suppress dissenting opinions at home. AI will also enable populists in democracies to politically corrode democratic and constitutional procedures as well as civil societies. Autocratic states are already using AI to exercise totalitarian dystopic control. Ideologies and religions are used as hybrid means, are becoming more important and are used to influence members of religious minorities. Secularisation is thus likely to decline worldwide. We can already say that political influence on religious communities will once more assume a more important role in the repertoire of geopolitical ambitions.

Military developments and technological innovations in the field of AI will increasingly affect societies outside the area of conflict, while the open AI arms race between the West and China will likely lead to profound AI-induced military and social upheaval. As discussed, non-state actors, too, will increasingly use such capabilities to pursue their political, ideological and economic goals. It is therefore necessary that Western countries take preventive measures to protect themselves. In its new National Security Strategy, Germany has already announced strategies to increase the capacity to act against and to counter hybrid threats as well as to deal with disinformation. We must use proactive research and development projects to maintain our current technological edge, to develop suitable protection and countermeasures such as forensic AI identification tools, and to enforce extensive bans on apps such as TikTok.

In future, the physical destruction of an adversary will no longer be the main focus, as it was in the first three generations of warfare. Future warfare will also not be primarily about attacking psychological warfare capabilities by decentralising force or influencing decision-makers, as was the focus of fourth-generation approaches. The non-kinetic approaches of fifth-generation warfare will become established in the long term as a central means of corrupting an enemy's society. The current trends and developments in hybrid threats will also lead to a manifestation of a sixth generation of warfare.

This generation will be all about the ability to control the space and time of an adversary's reality. For this currently emerging sixth generation of warfare, it is therefore essential to penetrate an adversary's military OODA loop (observe, orient, decide, act), for example. Instead of just disrupting the OODA loop as before, it is important to control it completely. Once it has been compromised, it is then possible to control what the adversary and their society see, hear and think. In this way, decisions of an opponent can be controlled and actions that appear rational to those taking them on the basis of the information available to them are used to one's own advantage. Thus, the projection of controlling the military OODA loop is extended to all other areas of society in order to guide government action, social preferences and positions as well as economic activities. As a result, modern societies will then be in a permanent hybrid state of war.

4 Rogue AI refers to an autonomous AI system that is no longer under human control. It can act in a way that could pose a threat to societies, the economy or the biosphere.

Metis

IMPRESSUM

Publisher

Metis Institute
for Strategy and Foresight

Bundeswehr University Munich

Web: metis.unibw.de

X: @metis_institut

Author

Dr. Konstantinos Tsetsos

metis@unibw.de

Creative Director

Christoph Ph. Nick, M. A.

zum-staunen.de

Image credits

Cover:
"Trojan horse in the digital age" | C. Nick,
motif created with the help of Midjourney.

Original title

Trends und Entwicklungen hybrider Bedrohungen

Translation

Federal Office of Languages

ISSN-2627-0609