Metis

Studie

Trends und Entwicklungen hybrider Bedrohungen

Nr. 35 | Juni 2023

Institut für
Strategie & Vorausschau

Zusammenfassung

Hybride Bedrohungen dringen in immer mehr Gesellschaftsbereiche vor. Hybrid agierende Akteure nutzen Verwundbarkeiten von komplexen und hochgradig vernetzten Gesellschaften aus, um politische, ideologische oder ökonomische Ziele durchzusetzen. Die vorliegende Studie widmet sich neuen Trends und Entwicklungen hybrider Bedrohungen und diskutiert zukünftige Implikationen für die nationale und internationale Sicherheit.

Fünf Generationen der Kriegsführung

Die ersten drei Generationen der Kriegsführung beziehen sich auf konventionell geführte Konflikte zwischen Staaten. Die von der Antike bis zum 19. Jahrhundert prädominante erste Generation (Formationskrieg) war von Linienkriegsführung mit schwerer Infanterie, dem Marsch in Kolonnen und Uniformierung geprägt. Verbesserte Präzision und Feuerkraft von Fernwaffen, Bahntransport und Motorisierung sowie eine zunehmende Industrialisierung der Kriegswirtschaft von 1850 bis 1930 dominierte die zweite Generation (Feuerkraft). Gesteigerte Feuerkraft manifestierte einen Stellungskrieg, so dass in der dritten Generation (Bewegungskrieg) verstärkt Taktiken zum Einsatz verbundener Waffen entwickelt wurden, die auf Geschwindigkeit und Überraschung setzten. Ziel war es, gegnerische Linien zu umgehen und die feindlichen Kräfte im Raum zu fassen. Bei den ersten drei Generationen lag der Fokus darauf, die feindlichen Streitkräfte physisch zu zerstören. Die vierte Generation (dezentrale Gewaltanwendung) ist darauf ausgerichtet, die psychische Fähigkeit eines Gegners zu unterminieren, indem Entscheidungsträger durch öffentlichen Druck zu politischen Entscheidungen gezwungen werden. Genutzt wird hierbei primär indirekte Kriegsführung durch Aufständische, um Opfer auf staatlicher Seite, vornehmlich demokratische Staaten mit niedriger Opfersensibilität, zu generieren. Die Zivilbevölkerung, öffentliche Meinung und Entscheidungsträger werden dadurch zum primären strategischen Schwerpunkt. Die Kriegsführung der fünften Generation (nicht kinetische Kriegsführung) wird in erster Linie durch *Social Engineering*, das Verbreiten von Fehlinformationen, Cyberangriffe sowie die Nutzung künstlicher Intelligenz (KI) und autonomer Systeme dominiert. Auch hier geht es darum, den Willen von Bevölkerungen und deren Entscheidungsträgern durch den Einsatz nicht kinetischer Mittel und unter Zuhilfenahme technologischer Innovationen zu beeinflussen. Alle oben beschriebenen Generationen sind als idealtypische Kriegsformen zu verstehen, die sich nicht gegenseitig ausschließen und auch gleichzeitig Anwendung finden können. Staaten sind heutzutage dementsprechend sowohl konventionellen als auch hybriden Bedrohungen, also komplexen und dynamischen Sicherheitsherausforderungen, ausgesetzt.[1] Zu den dabei verwendeten nicht traditionellen Mitteln gehören zum Beispiel Wahlbeeinflussung, ökonomische Schwächung, die planmäßige Verbreitung von Propaganda bis hin zu Cyberaktivitäten und Spionage.

Cyberangriffe, die kritische Infrastrukturen, Finanzsysteme oder Regierungsinstitutionen unterminieren und Desinformationskampagnen, die parallele Narrative zu etablieren suchen, nehmen seit Jahren zu. Bei einer Vielzahl hybrider Bedrohungen besteht zudem weiterhin das Attributionsproblem: Initiator und Verursacher sind nicht eindeutig zu bestimmen, was es erschwert, diese zur Verantwortung zu ziehen. Zudem dehnen sich die Angriffe von hybrid agierenden staatlichen und nicht staatlichen Akteuren auf weitere Gesellschaftsbereiche aus. Um die Transition von der vierten über die fünfte hin zur

1 Siehe „Neue hybride Bedrohungen", Metis Studie Nr. 26 (Juli 2021).

sechsten Generation zu verdeutlichen, werden im Folgenden einige aktuelle Trends und Entwicklungen neuerer hybrider Bedrohungen erörtert.

Aktuelle Trends bei Desinformation

Die Verbreitung von Desinformation, um gesellschaftliche Entscheidungsfindungsprozesse zu stören oder Wahlen zu beeinflussen, ist nicht neu. Die jüngsten Fortschritte bei der Entwicklung generativer KI für Texte und Bilder lassen aber eine nachhaltige Verbesserung bei Quantität und Qualität der Desinformation erwarten. Bisher waren beispielsweise Chatbots in sozialen Medien aufgrund ihrer qualitätsarmen Inhalte oder der minderen sprachlichen Qualität und repetitiven Argumentation relativ einfach zu enttarnen. KI-generierte Bilder konnten meist durch eine einfache Prüfung, beispielsweise durch das Auffinden von zusätzlichen Körperteilen, insbesondere Fingern, entlarvt werden. Auch KI-Videos und die Stimmenemulation bekannter Persönlichkeiten waren ohne forensische Mittel, beispielsweise durch mangelnde Lippensynchronisation oder Betonungsfehler, als Fälschung identifizierbar. Seit der Veröffentlichung generativer KI-Modelle Ende 2022 ist es jedoch möglich, mit nur wenigen Anleitungssätzen realistische Bilder, Texte und zeitnah auch Videos zu erstellen, die selbst auf den zweiten Blick nur schwer oder gar nicht mehr als Fiktion enttarnt werden können. Durch Sprachsynthese-Software und andere Techniken erzeugte Deepfakes wird die Kontrolle über das eigene Abbild zu einem Relikt der Vergangenheit, was öffentliche Debatten prägen und bestehende Datenschutzstandards aushebeln wird. Diskussionen zu politischen und sozialen Themen zwischen KI-Bots samt elaborierten Kommentaren werden für den durchschnittlichen Nutzer wie Debatten zwischen Expert*innen erscheinen und das öffentliche Meinungsbild mitbestimmen.

Social-Media-Plattformen als hybrides Mittel

Soziale Medien haben sich als moderne Informations- und Kommunikationsmittel etabliert und bestehenden Medienformaten Marktanteile abgenommen. Desinformation begleitete ihren Aufschwung von Beginn an. Staatliche Regulierungsmaßnahmen und von den Betreiberfirmen – abhängig vom jeweiligen nationalen Kontext – eingeführte Regeln versuchen durch Zensur, Filter, Community Feedback, Warnhinweise oder Account-Sperren etwa gewaltverherrlichende, rassistische oder sexistische Inhalte und offensichtliche Falschinformationen einzudämmen. Um diese Maßnahmen zu umgehen, greifen User wiederum auf weniger regulierte Messenger-Dienste wie Telegram zurück. Die US-Plattformen wie Google (YouTube), Meta (Facebook, Instagram, WhatsApp) oder Twitter verfolgen ein primär ökonomisches Interesse und erheben Nutzerdaten zu Werbezwecken.

Neuere Videodienste wie TikTok vom chinesischen Plattformbetreiber ByteDance stellen eine Evolution der hybriden Bedrohungen im Informationsbereich dar. Anders als bisher sind sie nicht nur Informationsschlachtfeld; die Plattformen selbst sind das hybride Mittel zur Einflussnahme. Die Betreiberfirma von TikTok ist aufgrund von Bedenken hinsichtlich des Daten- und Jugendschutzes sowie der Spionage und Zensur zugunsten der chinesischen Regierung weltweit in Kritik geraten. Sie ist kein rein privatwirtschaftlicher Anbieter mit Profitmaximierungsabsicht, sondern aufgrund der Nähe zur chinesischen Regierung ein semistaatlicher Akteur. Die App sammelt mehr Daten über Nutzer als vergleichbare Applikationen. Offiziell werden solche Daten zur Verbesserung von Algorithmen verwendet. Cyberexperten haben aber bereits in mehreren Fällen nachgewiesen, dass TikTok Hintertüren (sogenannte *Backdoors*) verwendet. Zudem verschleiert die App welche Daten erhoben werden und wohin sie gesendet werden. Auch verfügt TikTok über die Fähigkeit gezippte Dateien zu empfangen und *Executables* auszuführen. So könnte beispielsweise Malware unerkannt überspielt werden. Wenn Nutzer die höchsten Privatsphäre-Einstellungen auswählen, gaukelt die App die Übernahme dieser Konfiguration zwar vor, sendet aber im Hintergrund weiter Daten. Die Inhalte sind meist trivial und komisch und von den Nutzern selbst erstellt. Der Algorithmus ist jedoch so optimiert, dass er die Nutzer durch die kurzlebigen Videos individual-psychologisch täglich stundenlang in den Bann ziehen kann. Brisante politische Themen wie beispielsweise Videos zu Demonstrationen in Hongkong werden gezielt zensiert und durch triviale Inhalte ersetzt. Der Algorithmus erstellt ein psychologisches Profil der Nutzer und lernt langsam, wie er den Nutzer ablenken oder durch die Präsentation von Inhalten in eine bestimmte Denkrichtung leiten kann. Studien haben gezeigt, dass vor allem bei jungen Nutzern, die drei bis fünf Stunden pro Tag TikTok konsumieren, Gleichgültigkeit zu politischen, ethischen und sozialen Fragen, geringere Produktivität, sowie eine positivere Einstellung zu China nachweisbar ist. Dadurch stellt TikTok eine Art trojanisches Pferd dar, welches nicht nur als Datenkrake fungiert und psychologische Profile aller seiner Nutzer erstellt, sondern auch als Mittel zur Beeinflussung Verwendung findet. Das Ziel von TikTok scheint die unterschwellige Einflussnahme auf eine ganze Generation durch Trivialisierung und Ablenkung zu sein, um zukünftige gesellschaftliche Entscheidungsprozesse zu manipulieren. Anders als im Rest der Welt ist TikTok in China selbst unter dem Namen Douyin verfügbar. Hier ergibt sich ein radikal anderes Bild; die App ist eine auf Bildung, Technologie und schöpferische Tätigkeiten fokussierte Plattform, die Nutzer zu mehr Produktivität, Kreativität und Unternehmertum anzuspornen versucht.

Kirchen und religiöse Vereine zur hybriden Einflussnahme

Kirchen und religiöse Vereine werden zunehmend zur politischen Einflussnahme durch externe staatliche oder nicht staatliche Akteure eingesetzt. Innenpolitisch geht es dabei primär darum, bestimmte politische, ideologische oder soziale Positionen religiöser Minderheiten zu fördern, das Wahlverhalten zu beeinflussen oder Rechtsauffassungen mit Hilfe religiöser Begründungen durchzusetzen. Ziel ist es meist, einen gesellschaftlichen Zersetzungsprozess voranzutreiben, ein autoritäres Weltbild bei der Anhängerschaft zu etablieren und religiös konnotierte Gesellschaftsmodelle aus anderen Staaten zu verbreiten. In Deutschland wird seit Jahren beobachtet, wie radikale christliche, islamische oder sektenähnliche Verbände verfassungsfeindliche religiöse Ansichten durch gemeinnützige Vereine verbreiten. Empfängliche Gesellschaftsteile werden gezielt in karitativen und bildungsnahen Einrichtungen rekrutiert. Kritische Stimmen aus den eigenen Reihen werden unter Androhung von Gewalt ausgeschlossen, während Journalist*innen, die die Vorgänge untersuchen wollen, tätlich angegriffen werden. Ein immer größerer Teil der hybrid agierenden religiösen Vereine wird dabei direkt oder indirekt von staatlichen Institutionen im Ausland finanziert, unterstützt oder kontrolliert. Die Satzung von DITIB, dem Verein Türkisch-Islamische Union der Anstalt für Religion, sieht beispielsweise vor, dass der Beirat des Vereins als Vorsitzenden den Präsidenten des Amtes für religiöse Angelegenheiten der türkischen Republik zu ernennen hat. Seit 2016 ist zudem bekannt, dass Organisationen wie die *Revival of Islamic Heritage Society* aus Kuwait, die *Shaykh Eid Charity Foundation* aus Katar oder die *Muslim World League* aus Saudi-Arabien in Europa Moscheen und Einrichtungen von Salafisten finanzieren.

Auch auf internationaler Ebene ist ein Trend zur Nutzbarmachung religiöser Institutionen zum geopolitischen Macht- und Kontrollzuwachs zu erkennen. Als beispielsweise das Patriarchat von Konstantinopel, als spirituelle Führung der Orthodoxie, 2018 der ukrainisch-orthodoxen Kirche den autokephalen Status verlieh und damit ihre Unabhängigkeit von der russisch-orthodoxen Kirche anerkannte, wurde dies von Moskau als Anlass genommen, ein Schisma mit Konstantinopel auszurufen. Seitdem verstärkte der Kreml religiöse Einflussnahme in überwiegend orthodoxen Staaten und versucht die traditionelle Führungsrolle Konstantinopels zu übernehmen. Der offene Konflikt zwischen griechischer und russischer Orthodoxie ist daher nicht theologischer Natur, sondern Teil einer hybriden Kampagne im Kampf um die religiöse Führung innerhalb der Orthodoxie. Russland investiert über kremlnahe Spender hohe Beträge in der Mönchsrepublik Athos, um dort Einfluss auf die wichtigsten Klöster auszuüben. Auch wird versucht die Patriarchate in Alexandria, Antiochia und Jerusalem politisch und personell zu vereinnahmen, um Mehrheitsverhältnisse innerhalb der Ökumene zu generieren. In der Türkei werden seit 2018 immer mehr russische Geistliche mit türkischem Pass aktiv, um in Zukunft mit Hilfe der türkischen Regierung sicherzustellen, dass der nächste oder übernächste Patriarch von Konstantinopel voraussichtlich russischer Herkunft sein wird.[2] Dies wäre nicht nur der erste russisch-orthodoxe Patriarch seit Bestehen des 1600-jährigen Patriarchats, sondern auch ein politischer Erfolg Russlands globalen Ausmaßes.

Das sunnitische Saudi-Arabien verfolgt durch die Verbreitung des Wahhabismus und Salafismus ähnliche Aspirationen spiritueller Hegemonie und steht dabei in direkter Konkurrenz mit dem schiitischen Iran. Über die direkte finanzielle Unterstützung von religiösen Vereinen und Bildungseinrichtungen wird in Afrika, Asien und Europa wahhabitisches Gedankengut gefördert. Zu diesem Zweck sind in den letzten Jahren nicht nur höhere finanzielle Mittel bereitgestellt worden; es wurde auch mit einer Vielzahl neuer Kommunikations- und Verbreitungsmethoden experimentiert, um vor allem junge, gut ausgebildete Muslime für sich zu gewinnen. Bisher waren primär marginalisierte oder ausgegrenzte Personen Ziel von Informationskampagnen und Rekrutierung, oftmals innerhalb religiöser Einrichtungen. Innerhalb der letzten Jahre hat die salafistische Bewegung enorme Summen für soziale Medien als Instrument zur Ansprache von Studenten, jungen Berufstätigen, Akademikern und anderen gebildeten Muslimen ausgegeben. Salafistische Kanäle auf Facebook und YouTube haben teilweise mehrere Millionen Anhänger. Es ist wahrscheinlich, dass wenn sich die von Saudi-Arabien finanzierte monolithische Sicht des Islams stärker durchsetzt, radikale Kräfte in lokalen Gemeinschaften weiterhin einen fruchtbaren Boden für die Rekrutierung antreffen werden.

Autonomie und KI als Waffe

Bisher wurde KI vorwiegend bei der Datenverarbeitung (*Data Processing*) verwendet. Durch die Analyse großer Datenmengen und das Erkennen von Mustern kann KI militärische Informationen schneller verarbeiten und Empfehlungen für taktische und strategische Entscheidungen geben. Die gängige Devise lautet: Wer mehr und schneller Daten verarbeiten und somit rascher entscheiden kann, gewinnt. Der Russisch-Ukrainische

2 Wegen der sinkenden Zahl Orthodoxer in der Türkei gestaltet sich die Wahl eines qualifizierten Kirchenoberhaupts zukünftig schwierig. Erschwerend kommt hinzu, dass die Ausbildung von Priestern zurzeit in der Türkei vom Staat verboten wird, jedoch als Voraussetzung gilt. Das einzige verbliebene griechisch-orthodoxe Priesterseminar wurde 1971, als alle privaten Hochschulen verstaatlicht wurden, vom Staat geschlossen. Eine Wiedereröffnung wurde seitdem nicht umgesetzt. Theologen müssen daher im Ausland studieren, riskieren dabei allerdings, dass ihnen die türkische Staatsbürgerschaft entzogen wird.

Krieg verdeutlicht die zunehmende Bedeutung von *Processing Power* und den gesteigerten Wert von unbemannten Systemen für die Kriegsführung im 21. Jahrhundert.[3] Kommerzielle Drohnen dienen beispielsweise zur Aufklärung oder zur Übermittlung von Zielkoordinaten für die Artillerie. Die meisten dieser Systeme sind nicht autonom, Operateure müssen sie weiterhin steuern und aufgrund der in Echtzeit übermittelten Bild- und Videoinformationen entscheiden, ob und wann ein Ziel bekämpft werden soll. Kurz gesagt: Der Mensch drückt in diesen Fällen weiterhin „den Knopf". Als Autonomie in Waffensystemen wird hingegen die Übernahme von Funktionen durch die Maschine bezeichnet, wo zuvor menschliche Einflussnahme notwendig war – was insbesondere mit Blick auf die Zielbekämpfung kontrovers diskutiert wird. Es existieren bereits seit Jahrzehnten Waffensysteme mit Autonomie in den sogenannten „kritischen Funktionen". Dass Waffensysteme unter gewissen Umständen also Ziele selbstständig auswählen und auch bekämpfen, ist durchaus längst gängige Praxis, vor allem bei der Abwehr von anfliegender Munition wie beispielsweise Raketen, Artillerie- oder Mörsergranaten. Der Funktionsumfang von KI hat sich in den vergangenen Jahren aber enorm gesteigert, insbesondere bei der Objekterkennung, sodass die maschinelle Funktionsübernahme nunmehr im Begriff ist, in zahlreichen weiteren Operationskontexten Einzug zu halten, was ethische, rechtliche und sicherheitspolitische Fragen aufwirft.

Befeuert durch die russische Aggression und angesichts der systemischen Konfrontation zwischen den USA als Hegemon und China als Herausforderer hat aber bereits jetzt ein KI-Wettrüsten eingesetzt. In zukünftigen Kriegen wird KI daher nicht nur auf den Schlachtfeldern von morgen die Fähigkeiten und Präzision von kinetischen Wirkmitteln verbessern, sondern auch in selbstständig operierenden Systemen auftreten, die sich gegen Gesellschaften abseits des Kriegsgeschehens richten. KI wird kritische Infrastrukturen, neuralgische Verkehrs-, Logistik- und Energieversorgungssysteme, den Finanzsektor oder Verwaltungssysteme attackieren oder überwachen. Sowohl im Angriff als auch in der Verteidigung kritischer Systeme wird KI im Cyberbereich zum Einsatz kommen. In Zukunft wird die Devise lauten: Wer über die beste KI verfügt, gewinnt. Staaten, die in so einem KI-Wettrüsten zurückfallen, werden aufgrund ihrer Verwundbarkeiten und mangelnder Resilienz Einbußen in ihrer politischen und ökonomischen Bedeutung erfahren. Mit fortschreitender Entwicklung kognitiver KI gehen zudem Risiken eines Kontrollverlusts einher. Das Auftreten einer *Rogue-KI*[4] ist daher keine Frage des ob, sondern des wann.

Nutzung von Drohnen durch nicht staatliche Akteure

Die militärische Nutzung kommerzieller Drohnen im Russisch-Ukrainischen Krieg verdeutlicht auch die technologische Reife der derzeit am Markt vorhandenen Systeme. Es ist zu erwarten, dass die Lehren auch bei nicht staatlichen Akteuren gezogen werden. Massenangriffe auf militärische und staatliche Installationen oder das bereits vereinzelt stattfindende Ausspionieren von Kasernen und Verteidigungsanlagen durch hybride Akteure ist dadurch immer wahrscheinlicher. Auch der Einsatz von Drohnen gegen kritische Infrastrukturen, zum Ausspionieren von Sicherheitsmaßnahmen oder zur Erkundung von Drogen- oder Schmuggelrouten ist plausibel. Piraten werden zukünftig Drohnen einsetzen, um zu prüfen, ob Containerschiffe bewaffnete Sicherheitskräfte an Bord haben und dann entscheiden, ob sich ein Angriff lohnt. Radikale Klimaaktivisten könnten mit Drohnen Kohlekraftwerke oder Ölraffinerien ausspionieren, neuralgische Komponenten beschädigen oder gezielt Brände legen. Terrorangriffe mit Drohnen gegen startende und landende Flugzeuge wären bereits heute umsetzbar. Da moderne Drohnen voraussichtlich immer kleiner und immer leiser werden, wird deren Identifikation, Abwehr und Nachverfolgung schwerer möglich. Es ist zu vermuten, dass kritische Infrastrukturen zukünftig nur durch großflächige Flugverbotszonen und Störsender geschützt werden können.

Implikationen zukünftiger hybrider Bedrohungen – die sechste Generation der Kriegsführung

Wie oben beschrieben dominieren neue gesellschaftliche Tätigkeitsfelder sowie *Emerging Technologies* aktuelle Entwicklungen hybrider Einwirkung und Einflussnahme. Im Bereich der sozialen Medien und Desinformation werden zunehmend die Plattformen selbst zum Wirkmittel, während KI-gestützte Verfahren die Qualität und Glaubwürdigkeit von Falschinformationen verbessern. Während in Europa Debatten über die normative und rechtliche Kontrolle von KI sowie Aspekte des Datenschutzes im Zentrum stehen, werden KI-gestützte Systeme Autokratien dabei helfen, liberale Demokratien global zu untergraben sowie abweichende Meinungen im eigenen Land zu unterdrücken. Zudem wird KI in Demokratien Populisten in die Lage versetzen, demokratische und rechtsstaatliche Verfahren sowie

3 Siehe „Unbemannte Systeme: Rüstung, Kontrolle und Rüstungskontrolle", Metis Studie Nr. 28 (Juni 2022).

4 Eine *Rogue-KI* ist eine abtrünnige KI, also ein autonomes KI-System, dass sich der Kontrolle durch den Menschen entzieht. Sie kann sich dann in einer Weise verhalten, die Gesellschaften, Wirtschaft oder die Biosphäre gefährden würde.

Zivilgesellschaften politisch zu zersetzen. In autokratischen Staaten wird KI bereits jetzt herangezogen, um totalitäre dystopische Kontrolle auszuüben. Ideologien und Religionen werden als hybrides Mittel eingesetzt, nehmen an Bedeutung zu und werden zur Einflussnahme von Angehörigen religiöser Minderheiten genutzt. International ist dadurch ein Rückgang der Säkularisierung zu erwarten. Bereits jetzt lässt sich attestieren, dass politische Einflussnahme auf Religionsgemeinschaften im Repertoire geopolitischer Ambitionen wieder einen größeren Stellenwert einnehmen wird.

Militärische Entwicklungen und technologische Innovationen im Bereich der KI werden zunehmend Gesellschaften abseits des Konfliktgebiets betreffen, während der offene KI-Rüstungswettlauf zwischen dem Westen auf der einen und China auf der anderen Seite voraussichtlich zu tiefgreifenden KI-induzierten militärischen und gesellschaftlichen Verwerfungen führen wird. Wie besprochen werden auch nicht staatliche Akteure sich solche Fähigkeiten zunehmend zu Nutze machen, um ihre politischen, ideologischen oder ökonomischen Ziele zu verfolgen. Es ist daher notwendig, dass westliche Staaten bereits jetzt präventive Maßnahmen ergreifen, um sich zu schützen. In der neuen nationalen Sicherheitsstrategie hat Deutschland bereits Strategien zur Steigerung der Handlungsfähigkeit gegenüber und zur Abwehr von hybriden Bedrohungen sowie eine zum Umgang mit Desinformation angekündigt. Durch proaktive Forschungs- und Entwicklungsvorhaben gilt es einerseits den derzeitigen technologischen Vorsprung zu behalten und andererseits geeignete Schutz- und Gegenmaßnahmen, wie forensische KI-Identifikationstools zu entwickeln oder weitreichende Verbote von Apps wie TikTok durchzusetzen.

Zukünftig wird nicht mehr die physische Zerstörung eines Gegners wie bei den ersten drei Generationen im Vordergrund stehen. Auch wird es nur bedingt darum gehen die psychischen Fähigkeiten zur Kriegsführung durch Dezentralisierung der Gewalt oder die Beeinflussung der Entscheidungsträger, wie bei Ansätzen der vierten Generation, zu attackieren. Nicht kinetische Ansätze der fünften Generation werden sich langfristig als zentrales Mittel zur Zersetzung der Gesellschaft eines Gegners etablieren. Zudem führen die aktuellen Trends und Entwicklungen bei hybriden Bedrohungen zu einer Manifestation einer sechsten Generation der Kriegsführung.

Dabei geht es darum den Raum und die Zeit der Realität eines Gegners zu kontrollieren. Für die sich derzeit anbahnende Kriegsführung der sechsten Generation ist also elementar, dass beispielsweise in die militärische OODA-Schleife (*observe, orient, decide, act* also das Beobachten, Orientieren, Entscheiden und Handeln) eines Feindes eingedrungen wird. Anstatt wie bisher die OODA-Schleife nur zu stören, geht es darum diese vollkommen zu kontrollieren. Ist diese erstmal kompromittiert, kontrolliert ein Akteur, was sein Gegner und seine Gesellschaft sieht, hört und denkt. Dadurch können die Entscheidungen eines Kontrahenten gelenkt werden und Handlungen, die aus Sicht des Handelnden auf Grundlage der vorhandenen Informationen als rational erscheinen, zum eigenen Vorteil verwendet werden. Im Ergebnis wird die Projektion der Kontrollübernahme der militärischen OODA-Schleife auf alle anderen gesellschaftlichen Bereiche ausgeweitet, um so staatliche Handlungen, gesellschaftliche Präferenzen und Positionen sowie wirtschaftliche Tätigkeiten zu lenken. Im Ergebnis befinden sich moderne Gesellschaften dann in einem permanenten hybriden Kriegszustand.

Metis

IMPRESSUM

Herausgeber

Metis Institut
für Strategie und Vorausschau
Universität der Bundeswehr München
Web: metis.unibw.de
Twitter: @metis_institut

Autor

Dr. Konstantinos Tsetsos
metis@unibw.de

Creative Director

Christoph Ph. Nick, M. A.
c-studios.net

Bildnachweis

Titel: *Trojanisches Pferd im digitalen Zeitalter* | C. Nick, Motiv erstellt mit Hilfe von Midjourney.

ISSN-2627-0587