HYBRID INTELLIGENCE AS A CARRIER OF DISINFORMATION AND HYBRID THREATS IN CYBERSPACE

DOI: https://doi.org/ 10.37458/nstf.26.1.2
Review paper
Received: 23 October 2024
Accepted: February 20, 2025

Nikola Mlinac*

Abstract: Social networks have become powerful media and communication tools that provide adequate support to state actors in cyberspace when planning and execution of influence operations. In this context, new patterns in planning and conducting covert offensive information operations will be presented, where artificial intelligence systems used by social networks play a crucial role. On a tactical level, these systems are utilized to exploit users' personal data on social networks regarding their political, ideological, and religious beliefs, as well as tendencies towards violent extremism, radicalism and terrorism, to create hybrid threats. The main hybrid threat presented here is automated and anonymous disinformation that adapts to these beliefs and tendencies.

* Nikola Mlinac holds a LLM in social science in the scholarly field of law with a specific focus on international law. He earned his master's degree from the University of Split Law Faculty in 2012 with the thesis "Extending the continental shelf boundaries of Arctic states and energy resources in the Arctic Ocean." He received his doctorate from the University of Zagreb Faculty of Humanities and Social Sciences in 2022 with the dissertation "Social networks as a means of influence in hybrid conflicts" in the scholarly field of information and communication sciences.

Hybrid intelligence is depicted as a key factor that has enabled the use of this category of user data for the creation of hybrid threats in cyberspace.

The article aims to underscore that artificial intelligence systems used by social networks have enabled more effective exploitation of weaknesses in political and social systems based on personal data about the beliefs and tendencies of social media users who are not sufficiently aware of it. The application of hybrid intelligence has further complicated the counteraction and timely recognition, mitigation, and deterrence of the potential harmful consequences of hybrid threats.

Keywords: artificial intelligence systems, social networks, influence operations, cyberspace, social vulnerabilities, disinformation, hybrid threats.

Introduction

This article aims to demonstrate that machine learning, deep learning, recommendation algorithm systems and automated fake accounts (bots) constitute key artificial intelligence systems, whereby different cyberspace actors use social networks as tactical tools in providing support for influence operation planning and execution. The intention is to underscore that the political, ideological and religious beliefs, and principles and values of social network users as well as their affinities for different forms of violent extremism, radicalism and terrorism are of great importance to the aforementioned systems in the context of creating hybrid threats when it comes to pre-planned, covert and targeted offensive information-psychological operations.

Hybrid intelligence is considered the application of said artificial intelligence systems in creating automated and anonymous disinformation. Such disinformation is used

for the targeted creation of hybrid threats and steering them in desired directions. Such threats are not a novelty when it comes to resolving international disputes and conflicts. The novelty, rather, lies in the tools and possibilities for their creation as well as the increased complexity of their timely recognition and deterrence. Threats that are reinforced by hybrid intelligence in cyberspace are considered hybrid threats. The context of hybrid threats will primarily be presented within the information domain of confrontations between international state actors. In that context, hybrid threats will be presented through the utilisation of the aforementioned artificial intelligence systems and user data on social networks in order to exploit social vulnerabilities for the creation of such threats.

The application of the aforementioned artificial intelligence systems on social networks has, with the possibility of automated and anonymous offensive activity adapted to social vulnerabilities, brought about a paradigm shift in the planning and execution of covert offensive information operations. Such offensive activities have become anonymous and automated, with social networks and hybrid intelligence becoming tools wielded by state actors to implement their own policies in an efficient manner and, consequently, create hybrid threats. Target audiences may, in that context, include states, political decision-makers, the general population, communities, groups or individuals that use social networks to express their political, ideological and religious beliefs and tendencies towards different forms of violent extremism, radicalism and terrorism.

Hybrid conflicts are observed through continuous economic, social, political and security crises and situations which, as a rule, precede any hybrid warfare and primarily take place and are kept within cyberspace by creating hybrid threats, where – due to their many advantages – artificial intelligence systems used by social networks play a key role (Mlinac, 2022). In times like these, interfering in electoral processes is viewed as a major hybrid threat with potential strategic consequences. Hybrid warfare in considered as a means of resolving international disputes, where force of arms is applied only as a final resort (Mlinac, 2022).

The United States of America and the Russian Federation are seen as key actors which, at times of hybrid conflicts and hybrid warfare, use social networks and hybrid intelligence to create hybrid threats. The context of creating hybrid threats will be presented through the example and within the context of the continuous conflicts that preceded the ongoing war in Ukraine, where the United States and Russia employed social networks in different geographical areas to support their planning and execution of influence operations. The U.S. hybrid threats in the context of hybrid warfare will be exemplified by the 2015-2020 civil and proxy war in Syria, whereas those in the context of hybrid conflict will be illustrated through the examples of 2021-2022 influence operations in Central Asian states.

Russia's hybrid threats in hybrid warfare will be exemplified by the 2014-2015 military intervention in Ukraine, while hybrid conflict will be illustrated through the examples of interference in the 2016 U.S. presidential elections and the 2017-2018 parliamentary

elections in the Baltic states (Estonia, Lithuania and Latvia), as well as in France and Germany. These examples illustrate the role of artificial intelligence systems in cyberspace at the tactical level of offensive activity with potential and actual strategic consequences in terms of providing efficient support for planning and executing influence operations. Different levels of applying hybrid intelligence depended on the context of given operational, tactical and strategic goals (Mlinac, 2022).

The notion of hybridity in international conflicts and influence operations in cyberspace[1]

For the past roughly fifteen years, the academic, scientific, political and military/security communities have been using the term "hybridity" to describe international economic, social, political and security crises and upheavals that, in some cases, escalated into open armed conflicts. There are many examples of wars and conflicts where new information and communication technologies (ICTs) administered by the artificial intelligence (AI) systems used by social networks assumed a key role in providing adequate and efficient information support to the planning and

[1] The prefixoid cyber- is Greek in origin and designates anything associated with computer-generated virtual reality. This prefixoid is contained in the word cybernetics. Under the influence of English, this prefixoid now appears in the Croatian language as well, where it becomes the first element of many compound and hyphenated compound terms, but is sometimes also written as a word on its own. As the prefixoid *kiber-* fits better into the Croatian language system and given that, when borrowing foreign elements, preference is accorded to those coming from Latin and Greek over those originating in English, German, French and other living foreign languages, the recommendation is to use the word *kiberprostor* rather than the words or compounds *cyberprostor*, *cyber-prostor*, *cyber prostor*. Source: http://jezicni-savjetnik.hr/?page=4.

execution of influence operations (Tuđman, 2009, pp. 25-45 and p. 29).[2]

The AI systems used by social networks based on principles that disregard fundamental ethical and moral norms, but rather serve commercial interests, offer new possibilities in planning and creating various threats and contribute to the effective reinforcement of such threats through the dissemination of automated and anonymous disinformation which may additionally – if someone so desires – be tailored to political, religious and ideological preferences as well as specific categories of tendencies among target audiences (TAs), such as violent radicalism, terrorism and violent extremism.

Hybridity is not a novel concept. It emerged as far back as ancient times to depict the application of technological solutions to support conflict and warfare strategies (Popescu, 2015). Accordingly, the concept of hybridity indicates conflict and warfare tactics that are as old as the very phenomenon of conflicts and wars. The Western academic, scientific, political and military/security communities have reinvented the concept of hybridity to describe in the best possible manner the growing role of cyberspace and its related ICTs in the warfare model applied by Russia, first in its military intervention in Georgia in 2008 and then again in Ukraine in 2014-2015. However, the notion of hybridity appeared somewhat earlier in Nemeth's 2002 study entitled "Future War and Chechnya: A Case for Hybrid Warfare" (Nemeth, 2002). The author utilised

[2] In international conflict resolution and the information warfare theory, the term influence operations encompasses information operations, media operations, public diplomacy and public relations, where said components serve the purpose of their implementation.

the concept of hybridity to depict the dependence of combat effectiveness on the capacity to exploit cyberspace and new ICTs in the war waged by Chechen rebels against the Russian authorities.

Following the emergence of the first social networks – Facebook in 2004, YouTube in 2005 and Twitter in 2006 – it became clear that they could be used beyond the scope and purpose for which they were originally designed, i.e., connecting friends and families, pursuing business opportunities, sharing ideas and providing global networked communication. Thus, in many subsequent instances of armed conflicts and economic, social, political and security crises and upheavals, the aforementioned social networks proved to be efficient tools for achieving political goals.

The notion of hybridity in the form of "new old conflicts and wars" in cyberspace is viewed as, and understood to imply, any exploitation of the power of AI systems to manage and plan covert offensive information operations, where the planners and executors of such operations aim to utilise social network user personal data and AI systems to pursue political goals. Personal data primarily refers to the exploitation of the aforementioned political, religious and ideological beliefs as well as tendencies towards different forms of violent extremism, radicalism and terrorism. In the context of exploiting said systems and personal data, political goals can be recognised in interests in exerting a short- or long-term influence on

the outcomes of international economic, social, political and security crises and upheavals.[3]

We may say that hybridity in cyberspace is a term that basically describes the technological power of AI systems to exert influence, whereby different actors can, in the short or long run, efficiently shape or reshape value and belief systems and tendencies among their TAs in line with their own needs. Thanks to such possibilities, globally accessible social networks have become strong tactical influencing tools providing effective support in the planning and execution of offensive information operations.

Principal artificial intelligence systems used in planning and conducting offensive information operations on social networks

The principal artificial intelligence systems used to plan and conduct covert offensive information operations on social networks include, as mentioned earlier, machine learning, deep learning, recommendation algorithm systems and automated fake accounts (bots). Machine learning adds to the efficiency of such operations in that it helps their planners and executors by capturing huge amounts of personal data where it identifies "useful patterns and correlations among different data," on which basis it "draws conclusions on future behaviour and, in accordance with such conclusions, determines further human behaviour" (Crnčić, 2020, p. 29).

[3] Social networks largely defined the essence of cyberspace and met the expectations of military strategists as of the early 1990s, who saw the emergence of cyberspace as an opportunity to develop a new theatre of war where information and communication systems (ICTs) and computer technologies would be used to manage information in order to shape or reshape human thought and decision-making.

Machine learning provides a better and faster understanding of different situations, ensures greater precision, accelerates decision-making processes and, thus, complements human evaluation and prediction. Deep learning is used to predict desired outcomes. Machine learning and deep learning select TAs based on their value, belief and principle systems, tendencies, interests, motives, identified weaknesses and vulnerabilities, and recognise their decision-making drivers. Recommendation algorithm systems arouse user interest in, and – in the long run – focus their attention only on a specific set of information items, limiting their access to new knowledge, whereas bots ensure automated and anonymous dissemination of a limited set of data that suit the interests of attackers.

Owing to the above-described capabilities, AI systems have allowed cyberspace to accommodate new efficient patterns for planning and executing covert offensive information operations/psychological operations. New patterns of psychological operations have become globally accessible; they can be planned and executed at all influence levels, in individual, group and mass settings. The objectives of such activities outside the context of wars and armed conflicts may be directed towards the creation of disinformation and hybrid threats at local, regional or global levels. AI systems have enabled the automation and anonymity of offensive activity and its adaptation to social vulnerabilities. The immediacy, anonymity, automation and adaptation of activity with a view to generating desired processes (Nadler, Crain and Donovan 2018; Stoica 2020; RPA 2021) constitutes a new pattern of creating meta-propaganda, pseudo-events and pseudo-knowledge, that is, information superiority (Akrap

2011, p. 310.; Tuđman 2008, p. 13 and pp. 124-125; Tuđman 2013, p. 19).

Types of hybrid threats, critical social vulnerabilities and social network user data used to create hybrid threats in cyberspace

Due to a number of the aforementioned advantages offered by AI systems and because cyberspace is not adequately regulated by law, just as these AI systems are not adequately regulated by moral and ethical norms and such norms in any case do not provide adequate protection of user data on beliefs and preferences among social network users, cyberspace has become an ideal environment for social networks to grow into a powerful and efficient tool used to create disinformation and hybrid threats. In the context of the abuse of machine learning, deep learning, recommendation algorithm systems and bots for the creation of efficient disinformation and hybrid threats, we can recognise the tactical and strategic benefits offered by such systems in their planning and execution.

The tactical benefits are reflected in the fact that AI systems can expose social network users to constant, automated and anonymous disinformation which, when this is in someone's interest, may accordingly be tailored to their political, ideological and religious beliefs as well as tendencies towards terrorism and violent radicalism and extremism. This opens possibilities for AI systems to use the aforementioned social network user data to create disinformation and hybrid threats in the pursuance of political agendas.

The utilisation of user data and AI systems to create disinformation and hybrid threats constitutes a major novelty in the shifting paradigm of international conflicts and wars. Specifically, the concept of hybrid threats implies a reality whereby actions and processes at the tactical level can yield significant results at the strategic level (Akrap and Mandić, 2020, p. 14). This key paradigm shift in offensive activity has been driven by AI systems. These systems have made it possible to identify social vulnerabilities based on social network user preferences and tendencies, and to tailor disinformation accordingly. By following that pattern, they have increased the efficiency of offensive activities through hybrid threats. It is also worth noting that their efficiency in hybrid conflicts relies on the technological exploitation of social vulnerabilities identified by AI systems through political, ideological and religious beliefs among social network users as well as their tendencies towards terrorism and different forms of violent radicalism and extremism. This fact is best reflected in the definition of hybrid threats "as a set of potential manifestations of particular hybrid operations which entail targeted and organised action towards a TA in order to exploit (incite, deepen) existing and create new vulnerabilities and foster feelings of division, insecurity, defeatism, powerlessness, hopelessness, ambiguity, suspicion, disruption and collapse of democratic structures and processes as well as the attenuation and control of the defence system" (Akrap, 2019, pp. 37-39).

The exploitation of user data on political, ideological and religious beliefs and tendencies towards terrorism and different forms of violent radicalism and extremism as well as the use of AI systems to identify social

vulnerabilities based on the described category of user data within a targeted political or social setting constitute the aforementioned key paradigm shift in offensive information and psychological activity in cyberspace. Owing to this capability, the aforementioned AI systems, which manage information operations on social networks as part of international conflicts, offer state actors efficacy in providing information support when planning and executing influence operations.

Table 1. Basic types of hybrid threats and the purposes for their creation in the context of influence operations (Heap, Hansen and Gill, 2021. pp. 10-11).

TYPES OF HYBRID THREATS	BASIC OBJECTIVES OF HYBRID THREATS
EXERTION OF INFLUENCE ON PUBLIC OPINION	Implies establishing, funding and supporting academic, educational and cultural institutions, traditional and non-traditional media channels with a view to exerting direct influence on a TA; creating and disseminating misinformation and disinformation.
DEEPENING SOCIETAL DIVISIONS	Implies funding, supporting or promoting national, religious or political and extremist organisations; polarisation of political debates to subvert a specific policy programme; exploitation of ethnic or cultural identities to undermine social cohesion.
AGITATION AND CIVIL UNREST	Agitation of targeted social, cultural, religious or ethnic groups to initiate protests in order to trigger specific policy changes in target states; disruption of political or economic processes by organising protests or boycotts; increasing the risk of radicalisation or violent escalation in target societies.
INTERFERENCE IN ELECTORAL PROCESSES	Implies interference in electoral processes in other states to influence the electorate's behaviour and decisions.
DECREASING THE TA'S TRUST IN GOVERNMENT AUTHORITIES	Implies discrediting and decreasing the TA's trust in executive, legislative and military authorities and other government bodies and public institutions to undermine the credibility and legitimacy of their policies.
UNDERMINING GOVERNANCE AND	Foreign state sponsorship of political parties or leaders; developing criminal networks and organised crime.

GOVERNMENT FUNCTIONS IN TARGET STATES	
ECONOMIC LEVERAGE	Increasing economic or energy dependency; use of sanctions or incentives with a view to a targeted weakening of the target state's economy.
INFLUENCE OPERATIONS IN CYBERSPACE	Implies continuous technological attacks in order to disrupt communication flows and the functioning of digital infrastructure as well as psychological attacks in order to reshape the TA's beliefs in the short or long run.
INCITEMENT TO TERRORISM AND VIOLENT EXTREMISM	Implies incitement to religious and political extremism and terrorism, organising ethnically motivated violence and encouraging the escalation of socio-political protests and sectarian violence.
EXPLOITATION OF TERRITORIAL DISPUTES	Implies creating separatist regions and supporting separatist movements to undermine regional political and social stability.

Table 1 shows different hybrid threats that can be enhanced by disinformation using UI systems at the tactical operational level. By presenting different types of hybrid threats, the intention is to further clarify the key advantages offered by the described AI systems at the tactical level when it comes to creating such threats: Machine learning and deep learning facilitate insight into political, ideological and religious beliefs as well as tendencies towards terrorism and other forms of extremism and radicalism. This insight is instrumental in the identification of the societal divisions and vulnerabilities to which information attacks are tailored, adjusted and directed. Recommendation algorithm systems allow for the selection of TAs that harbour the desired beliefs and tendencies, while bots increase the visibility of disinformation to such TAs.

The strategic advantages offered by AI systems at the above-described tactical level of application are reflected in the fact that automated, anonymous and

customised disinformation can, in the short or long run, create new or reinforce existing social vulnerabilities according to which hybrid threats are defined and adjusted in terms of their intensity and scope.

Table 2 aims to further stress the security context of using AI systems and social network user data in creating hybrid threats. The security context of utilising the aforementioned user data on the TA's beliefs and tendencies in order to create hybrid threats outside the war setting comes into focus mostly during electoral campaigns at different levels, when it may have far-reaching consequences. My intention is to point out that the use of AI systems has a very negative security context because, in order to create hybrid threats, they utilise the personal data of social network users who reveal their political, religious and ideological preferences and tendencies towards extremism, radicalism, terrorism, political parties, specific ideas and ideologies. The table is meant to place additional emphasis on the security context of abuse of this category of personal data.

Based on such data, and by applying hybrid intelligence in covert psychological operations, which are – in the context of international conflicts – normally planned and conducted by specialised state-controlled military and civilian intelligence structures or different non-state actors under the control of state structures, disinformation and hybrid threats can be adjusted depending on the objectives of a given offensive activity. When there is a need to deepen the existing or create new hybrid threats, e.g. to incite or deepen the distrust of targeted socio-political groups in government authorities or to undermine security

stability by inciting street riots, organising protests or mobilising supporters of radical and extremist groups, or to incite terrorist activities and aspirations, anonymous disinformation will be targeted at social network users with opposing ideological, religious or political beliefs as well as those propagating radicalisation, extremism and terrorism.

Machine and deep learning identifies tendencies among such individuals and groups, recommendation algorithm systems reinforce their cognitive biases, while bots increase, in an automated manner, the visibility of information items that social network users, as the TA, "want to see." For instance, by using this model, the level of a society's radicalisation is artificially increased, while disinformation and information items are tailored so as to enable those conducting such operations to (re)shape the TA's knowledge of a particular socio-political event and to steer their future decisions and behaviour in directions as desired by the attacker. Regardless of the existence of physical boundaries, potential TAs for information attacks by disinformation have come to include all social network users whom influence operation planners can involve in a certain conflict at their own discretion (Mlinac, 2022).

Table 2. Critical social vulnerabilities, critical social network user data and key periods for the creation of disinformation and the planning and execution of hybrid threats in the context of influence operations.

CRITICAL SOCIAL VULNERABILITIES	CRITICAL SOCIAL NETWORK USER DATA	KEY PERIODS
clashes between government and opposition over political views; societal divisions on various grounds (ethnic, religious, political, economic or ideological differences); differing interpretations of historical events; corruption scandals; government inefficiency in law enforcement.	tendencies towards violent extremism, radicalism and terrorism; religious and political beliefs; tendencies towards ideologies.	peace, crisis and post-war periods; electoral political campaigns.

Hybrid intelligence and social networks as carriers of hybrid threats

The previously described context of creating hybrid threats by means of disinformation using AI systems and social network user personal data is viewed through the concept of hybrid intelligence. Hybrid intelligence, sometimes also called augmented intelligence, emphasises the assistive role of machine learning and other data-driven techniques which enhance human intelligence (just as telescopes enhance human vision), rather than replace it (van der Aalst 2021, p. 9). Dellermann et al. define hybrid intelligence "as the ability to achieve goals by combining human and artificial intelligence, thereby reaching superior results to those each of them could have accomplished separately, and continuously improve by learning from each other" (van der Aalst, 2021, p. 9.).

However, its application on social networks in order to create disinformation and hybrid threats has acquired strong negative security connotations. The power of

hybrid intelligence is reflected in the fact that machine and deep learning, based on automated predictive analytics and structured data on social networks, identifies the TA's critical psychological drivers, such as political preferences and tendencies towards terrorism, radicalism and extremism. Such knowledge provides the planners and executors of covert offensive information operations with greater insight into social vulnerabilities, which are – when this is in someone's interest and if someone so desires – used as a mould to shape disinformation and reinforce hybrid threats through its mass, automated and anonymous dissemination in the public and media space.

The key factors which facilitated abuse of hybrid intelligence to create disinformation may be recognized in the aforementioned aspects: inadequate regulation of cyberspace, inadequate protection of social network user personal data, such as beliefs and preferences, and the absence of adequate ethical and moral norms that would curb the abuse of the above-described AI systems. Due to the lack of adequate rules and the automation and anonymity of activity, hybrid intelligence has additionally lowered the threshold for timely recognition of disinformation and hybrid threats because they are tailored to values, beliefs and principles, i.e. to what TAs "want to hear and see." Global connectivity in cyberspace, the inadequate regulation of AI systems operating therein and immense quantities of structured personal data have, despite the existence of physical boundaries, led to a situation wherein all social network users become potential targets whose user data can be utilised to create hybrid threats.

The aforementioned patterns of offensive information operations by means of anonymous and automated disinformation are, in practice, executed continually in times of peace and crises and in post-war periods, using the noted social vulnerabilities and susceptibility of TAs to external influences. Such information attack patterns entail ongoing adjustments to the identified weaknesses of TAs and their resilience to external economic, social, political and security crises. The social vulnerabilities that have the greatest value for creating hybrid threats by means of disinformation include clashes between governmental authorities and the opposition over different policies, existing social divisions on various grounds (ethnic, religious, political, class-related, economic or ideological differences, or differing interpretations of historical events), corruption scandals and a government's inadequate law enforcement capability (see Table 2). These threats and social vulnerabilities have been around since time immemorial, but what makes them different in globalised cyberspace is reflected in the fact that thanks to social networks they are wielded in a targeted, automated and anonymous manner at systemic weaknesses in order to further undermine the TA's social and political cohesion.

Hybrid threats in the context of hybrid conflicts and hybrid warfare

Examples of using hybrid intelligence and social network user data on political, religious and ideological beliefs and tendencies towards violent forms of radicalism and extremism as instruments to create hybrid threats are examined primarily in the context of hybrid conflicts, i.e. continued economic, social,

political and security crises. While some examples of hybrid warfare are presented as well, the aim is to highlight the prevalence of factors that clearly point to the evident trend of using hybrid intelligence on social networks in order to achieve political goals (Mlinac, 2022). Standing out in this context are five confirmed examples of covert psychological operations on Russia's part and two confirmed examples of such operations on the part of the USA, where – depending on their strategic, operational and tactical goals and requirements – the two actors carried out the operations in cyberspace by using hybrid intelligence on social networks to create hybrid threats within the context of supporting other components of influence operations.

Russia's hybrid threats exemplified by the 2014-2015 hybrid war in Ukraine and U.S. hybrid threats exemplified by the 2015-2020 civil and proxy war in Syria

In the example of the 2014-2015 hybrid warfare in Ukraine, Russia used social networks at a tactical level to create a series of hybrid threats. Relying on social networks in cyberspace, it provided information and psychological support to its efforts to boost separatist movements in Crimea and separatist tendencies in the country's eastern provinces, disrupted the cohesion of Ukrainian society and political structures, and undermined the overall efficiency of governance and the adoption of quick and adequate countermeasures by the Ukrainian authorities (Mlinac, 2022). To this end, it used social networks to create and disseminate disinformation and reinforce hybrid threats in more efficient (automated and anonymous) ways.

By means of social networks, it effectively exploited existing ethnic and cultural tensions, steered protests towards escalation, undermined the credibility of Ukraine's government and armed forces to give legitimacy to its activities, recruited fighters, and mobilised the TAs according its needs and interests. Russia's 2014-2015 hybrid warfare model in Ukraine demonstrated that social networks could be used as tools in cyberspace warfare operations enabling efficient tactical and operational planning and execution of multiple threats with strategic consequences (Mlinac, 2022). The strategic consequences of the described offensive activity through hybrid threats are reflected in reducing Ukraine's overall capabilities to counter military intervention, the annexation of Crimea and the stay of Russia's Black Sea Fleet in Crimea. The most important issue was to prevent NATO from expanding to Ukraine (Mlinac, 2022).

The civil war in Syria is the only example from the Arab Spring process where hybrid threats escalated into an overt proxy war (Baezner and Robin, 2017). The civil and proxy war in Syria initially involved numerous armed proxy groups that fought each other through local religious communities and were, on the one hand, backed by Iran and Lebanon and, on the other, by Saudi Arabia, Turkey and Qatar. Via these two blocks of rival regional states, Syria hosted a conflict between the geopolitical and economic interests of the United States and Russia. Later these two key actors themselves became involved in hostilities through their own armed forces. The civil and proxy war in Syria provided an illustrative example of external, internal and proxy actors using cyberspace

and social networks to create hybrid threats in an unprecedented manner (Mlinac, 2022).

At the tactical level, the actors utilised relevant social network user data on political, ideological and religious beliefs and tendencies towards radicalism and extremism depending on their own strategic needs. All of the involved actors conducted cybertechnological incursions into protected information systems and adversarial information and communication systems to disrupt online services and gather tactical intelligence data in order to maximise the efficacy of military operations. The quality of these technological attacks was limited, but they were quite extensive. During the armed conflict, hybrid intelligence was less represented in creating disinformation. All of the involved actors used social networks to gain information superiority by placing their own announcements and news. Certain actors fostered multiple different hybrid threats to counter Russia's cyberspace influence operations and its policies, especially to curb the activity of Russia's naval forces in the Eastern Mediterranean.

Hybrid threats exemplified by Russia's interference in the 2016-2019 EU and 2016 U.S. electoral processes

In the 2018-2019 parliamentary elections in Lithuania, Estonia and Latvia (Backes and Swab 2019), the 2016-2017 parliamentary elections in Germany and France (Baezner and Robin 2017.) and the 2016 presidential elections in the United States (Aceves, 2019; Walker 2019.), the main hybrid threat was interference in electoral processes. In these examples, Russia used social networks and hybrid intelligence to provide adequate information support in cyberspace for other

components of influence operations that were, in the context of public diplomacy efforts, aimed at countering U.S. and NATO policies.

During the parliamentary elections in Lithuania, Estonia and Latvia, rather than creating new divisions within these societies, Russia took advantage of the sensitive political, ethnic, social and economic issues that already existed and divided the populations of the Baltic states, undermined the credibility of their institutions, advanced pro-Russian political forces and strived to create domestic instability, all with the long-term objective of furthering Russian interests. In the example of interference in elections in Germany and France, Russia undertook offensive activities at a strategic level in an effort to undermine the credibility of political party leaders who favoured NATO policies and the imposition of sanctions against Russia over the annexation of Crimea. In the example of interference in the U.S. presidential election, Russia used Facebook and Twitter to create various hybrid threats: it fomented existing racial, class and other social divides. To these ends, it used five basic categories of social and political problems: racial identity, immigration policy, police brutality, minority rights and the right to bear arms, as well as other, similar issues that provoke divisions and conflicts in U.S. society. One of the tactics was to use Facebook and Twitter posts to foster additional tension between supporters of liberal policies and ideologies and proponents of radical right views, place them in direct confrontation with each other and, in some cases, organise street clashes.

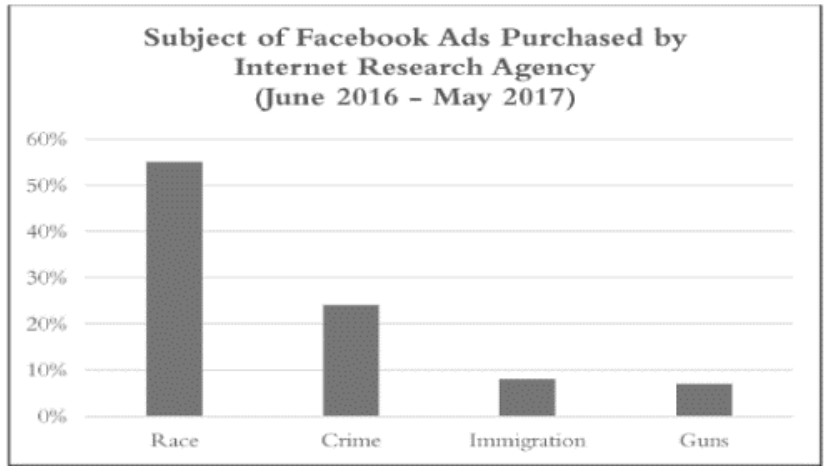

Figure 1. Chart showing key U.S. social vulnerabilities used by Russia to create hybrid threats via Facebook ads during the 2016 U.S. presidential election campaign. The data refer to the period from June 2016 to July 2017 (Mlinac, 2022).

Source: Aceves, "Virtual Hatred: How Russia Tried to Start a Race War in the United States," 2019, p. 193.

Figure 1 shows that in order to create hybrid threats, 55% of the ads exploited beliefs on racial identity, 23% relied on tendencies towards crime, 8% targeted beliefs on immigration policies, whereas 6% focused on opposing positions on the legitimacy of laws allowing the use of firearms in certain states. Based on the relevant data, AI systems identified major social vulnerabilities within U.S. society. The attacker took advantage of these vulnerabilities to plan and carry out covert psychological operations whereby it created hybrid threats in terms of influencing public opinion, deepening social divisions, inciting civil unrest and undermining the TA's trust in the government.

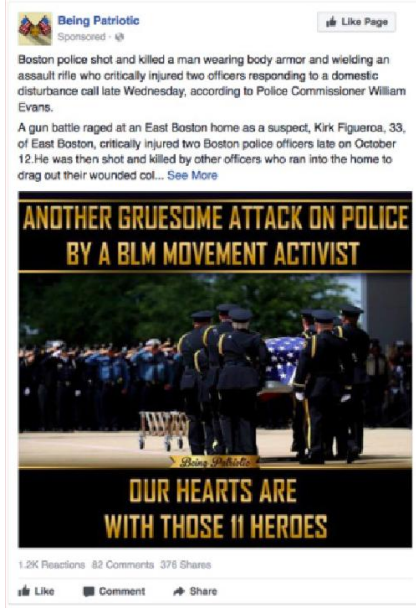

Figure 2: The appearance and content of the ad placed via the fake Facebook group account called "Being Patriotic."

Source: Nadler, Crain, Donovan, "Weaponizing the Digital Influence Machine," 2018, p. 31.

Figure 2 shows the appearance and content of the ad placed via the fake Facebook group account called "Being Patriotic," through which Russia's hacker organisations tried to mobilise right-leaning U.S. voters advocating the dignity of the police. The purpose of the ad was to create disinformation in order to place blame for an actual attack against a police officer on members of the non-governmental organisation Black Lives Matter, which gathered black communities inclined to liberal policies. Such ads were used to create hybrid threats aimed at inciting violent extremism, deepening social divisions, stirring up civil unrest and violence between groups with opposing political beliefs, and

encouraging individuals and groups to foster tendencies towards violent extremism and radicalism.

The strategic consequences of exploiting user data on beliefs and tendencies at a tactical level were reflected in shaping or reshaping political beliefs, principles and values among different TA categories within the U.S. electorate, creating a perception of external influence on the election of a new U.S. president, provoking doubts in the current administration's competence, and fomenting distrust of U.S. governmental institutions. One of the key issues was to limit its foreign policy influence inside Russia's spheres of interest in Europe (Cohen and Bar'el, 2017, p. 47).

2021-2022 U.S. hybrid threats in Central Asian states

By means of social networks, the U.S. created hybrid threats in Central Asian states and used them in cyberspace to provide information support for other influence operation activities in line with its predefined tactical, operational and strategic objectives (Unheard Voice, 2022). In the context of pursuing public diplomacy objectives and media operations, an increase in the number of fake social network accounts was visible on three occasions: in the period prior to the signing of the U.S.-Taliban Agreement for Bringing Peace to Afghanistan in February 2020, in the period leading to the departure of the U.S. armed forces from Afghanistan in August 2021 and at the beginning of Russia's military intervention against Ukraine in February 2022 (Unheard Voice, 2022).

For the purposes of shaping and reshaping the TA beliefs in Central Asian states, social networks provided the U.S. with certain basic tactical advantages,

including the division of TAs by country, where hybrid threats, in terms of their intensity, mostly focused on the TAs in Kazakhstan and Afghanistan in accordance with different approaches to achieving the defined tactical, operational and strategic objectives (Unheard Voice, 2022, p. 2).[4] In the period from August 2021, the TAs in Afghanistan were exposed to hybrid threats in order to shape and reshape their beliefs regarding the reasons behind the departure of the U.S. forces from Afghanistan. The TAs in Kazakhstan mostly included Russian-speaking communities in order to shape and reshape their beliefs on the reasons behind Russia's military intervention against Ukraine in accordance with U.S. public diplomatic activities and media operations.

At a tactical level, in both cases the U.S. resorted to the use of social networks to pursue the delineated goals of its influence operations due to the benefits of their automation and anonymity. Hybrid intelligence was used in order to select TAs and tailor hybrid threats to identified social vulnerabilities. As already mentioned, the anonymity of hybrid threats implied the coordinated use of fake profiles on different (Western and Russian) social networks whereby original press releases from U.S. diplomatic missions in Central Asian states were shared, as well as those from the U.S. media channels.

Social network anonymity was additionally used at a tactical level to deepen existing social vulnerabilities, divide the TAs in the target states into pro- and anti-government sympathisers, incite the TAs to socio-

[4] The study in question also includes examples of shaping and reshaping the TA beliefs in Turkmenistan, Uzbekistan, Kyrgyzstan, Tajikistan, Syria, Kuwait, Lebanon, Yemen, Iraq and Iran. However, these examples are not subject to any in-depth research.

political activism for self-gain and to launch fake petitions aimed at boycotting the Russian media.

In case of Kazakhstan, the major hybrid threats included efforts to undermine confidence in governmental authorities so as to erode the credibility and legitimacy of Kazakhstan's current policies towards membership in the Collective Security Treaty Organisation, which was initiated by Russia.[5] In order to reinforce hybrid threats, use was made of different social vulnerabilities: corruption, economic underdevelopment, crisis situations such as food shortages, differences in living standards and the government's inadequate law enforcement. These social vulnerabilities were also used to provide information support to anti-government and subsequent pro-Ukrainian protests provoked by Russia's military intervention against Ukraine in 2022. At a strategic level, the described tactical activities were aimed at additionally advancing U.S. foreign policy objectives, undermining the credibility and legitimacy of policies that advocated pro-Russian positions, disrupting cohesion within foreign-policy, economic and military security organisations such as the Commonwealth of Independent States, the Eurasian Economic Union and the Collective Security Treaty Organisation.

[5] For more details, see Organizacija Sporazuma o kolektivnoj sigurnosti. *Hrvatska enciklopedija, mrežno izdanje.* Leksikografski zavod Miroslav Krleža, 2021. Accessed on 28 April 4 2023. http://www.enciklopedija.hr/Natuknica.aspx?ID=71309

Figure 3: The appearance and content of the fake Facebook page that used the hashtag #CentralAsiaforUkraine (in the Russian language) to display Kazakhstan's support for Ukraine.

Source: "Unheard Voice, Evaluating five years of pro-Western covert influence operations," Graphika, Stanford Internet Observatory, Cyber Policy Center, USA, 2022, p. 19.

Figure 3 shows the appearance and content of a post shared via the fake Facebook group account called "Pulse of the East," whereby the U.S. created different types of hybrid threats such as exerting influence on public opinion, undermining trust in governmental authorities, inciting civil unrest and deepening social divisions.

Conclusion

Given the nature and objectives of influence operations, social networks have grown into a powerful and efficient influencing tool used by different actors in international conflicts primarily to create hybrid threats.

The artificial intelligence systems used by social networks, as well as personal data on the beliefs and tendencies of their users, have become key instruments for creating such threats. This paper aims to underscore that in the context of creating hybrid threats a key role is played by personal user data whereby social network users exchange views and opinions on political, religious, ideological and other beliefs or share their extreme, radical positions and information on various social and political circumstances. Since the aforementioned personal data constitute a crucial category underpinning the operation of social networks, they are not adequately protected, which is why different actors – both state and non-state – often use or abuse such data to pursue their political goals.

Such goals can, of course, include the creation of hybrid threats within different scopes of offensive information activities. The objective of hybrid activity by means of such threats has been examined primarily through the possibilities of using AI systems to undermine the social and political cohesion of a particular political system or social structure with a view to imposing other ideas and policies as acceptable and desirable.

As demonstrated in the paper, due to a number of advantages owing to which social networks have left the management of information operations to AI

systems, within the context of international conflicts this category of operations has assumed the characteristics of covert psychological operations that can be planned and carried out locally, regionally and globally, in an anonymous and automated manner, and with maximum flexibility to suit social network users as individuals or groups. Before the emergence of social networks, such operations were normally planned and carried out by specialised state-controlled military and intelligence structures. After the emergence of social networks, besides state structures they may be planned and carried out by different non-state actors that may or may not be under state control.

The rules dictated by social networks in cyberspace have become a crucial weakness exploited by state actors to make more efficient use of certain social vulnerabilities in order to create hybrid threats. The objective of hybrid threats is to achieve political goals. In the context of international conflicts, the purpose of hybrid threats is to redesign the conflict and steer it into the desired direction with a view to creating a series of cumulative negative effects on social and political stability in the geographical zone of the attacker's interest.

A comparative analysis of covert psychological operations conducted by Russia and the United States as part of their influence operations in different geographical areas has put in focus different hybrid threats whose planning and implementation at the tactical level involved the use of social networks by both actors in an effort to potentially achieve their strategic objective: disrupting social and political cohesion within their opposing military, economic and

security alliances. At the tactical level, the described information and psychological activities differed in terms of their intensity, preparation levels and duration, which – in that context – entailed differences in the scope and intensity of using hybrid intelligence to create hybrid threats.

Literature:

1. Akrap, Gordan (2011). Informacijske strategije i operacije u oblikovanju javnog znanja, Doktorska disertacija, Sveučilište u Zagrebu Filozofski fakultet, Zagreb.
2. Akrap, Gordan (2019). Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura: Strategos: Znanstveni časopis Hrvatskog vojnog učilišta "Dr. Franjo Tuđman", Zagreb.
3. Akrap, Gordan; Ivica, Mandić (2020). Why Security Science, Security Science Journal, Zagreb, Vol. 1 No. 2.
4. Akrap, Gordan (2023). Hibridne prijetnje i izazovi, Operacije utjecaja i moderno – sigurnosno okružje, Hrvatska sveučilišna naklada, Sveučilište u Mostaru.
5. Aceves, William J. (2019). Virtual Hatred: How Russia Tried to Start a Race War in the United States, The Michigan Journal of Race and Law, California Western School of Law, SAD Vol. 24 (2).
6. Baezner, Marie; Robin, Patrice (2017). Hotspot Analysis: Cyber and Information Warfare in elections in Europe, Center for Security Studies, Zürich.
7. Baezner, Marie; Robin, Patrice (2017). Hotspot Analysis: The use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict, Center for Security Studies, Zurich.
8. Backes, Oliver, Swab, Andrew (2019). Cognitive Warfare The Russian Threat to Election Integrity in the Baltic States, Belfer Center for Science and International Affairs Harvard Kennedy School.
9. Cohen, Daniel; Bar'el, Ofir (2017). The Use of Cyberwarfare in Influence Operation, Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University.

10. Crnčić, Saša (2020). Umjetna inteligencija u poslovanju, Diplomski rad, Sveučilište Sjever.
11. Heap, Ben; Hansen, Pia; Gill, Monika (2021). Strategic Communications Hybrid Threats Toolkit, Applying the principles of NATO Strategic Communications to understand and counter grey zone threats, NATO Strategic Communications Centre of Excellence, Riga, 10-11.
12. Hrvatska enciklopedija, mrežno izdanje. Accessible at: https://www.enciklopedija.hr/impresum.aspx
13. Mlinac, Nikola (2022). Društvene mreže kao alati utjecaj u hibridnim sukobima, Doktorska disertacija, Filozofski fakultet, Sveučilište u Zagrebu.
14. Nadler, Anthony; Crain, Matthew; Donovan, Joan (2018). Weaponizing the Digital Influence Machine, Data & Society Research Institute, USA.
15. Nemeth, William J. (2002). Future war and Chechnya: a case for hybrid warfare, Monterey, California, Naval Postgraduate School, USA.
16. Popescu, Nicu (2015). Hybrid Tactics: Neither New Nor Only Russian, The European Union Institute for Security Studies.
17. Robotic Process Automation (2021). RPA in Advertising | Social Media, Data Management.
18. Stoica, Aurelian (2020). From Social Influence to Cyber Influence. The Role of New Technologies in the Influence Operations Conducted in the Digital Environment, International Journal of Cyber Diplomacy.
19. Tuđman, Miroslav (2008). Informacijsko ratište i informacijska znanost, Hrvatska sveučilišna naklada, Zagreb.
20. Tuđman, Miroslav (2009). Informacijske operacije i mediji ili kako osigurati informacijsku superiornost', National security and the future, Zagreb.
21. Tuđman, Miroslav (2013). Programiranje istine, Rasprava o preraspodjelama društvenih zaliha znanja, Hrvatska Sveučilišna zaklada, Zagreb.
22. Unheard Voice, Evaluating five years of pro-Western covert influence operations (2022). Graphika, Stanford Internet Observatory, Cyber Policy Center, USA.
23. Van der Aalst, W.M.P. (2021). Hybrid Intelligence: to automate or not to automate, that is the question,

International Journal of Information Systems and Project Management.

24. Walker, Robert (2019). Combating Strategic Weapons of Influence on Social Media, Homeland Security Digital Library, USA.