THE DEFENCE HORIZON JOURNAL

Aspects of Cognitive Warfare

Masterhead

The Defence Horizon Journal is a professional and academic journal that features essays, reports, and analyses covering geopolitics and law, security- and defence policy, peace and conflict studies, applied military science, as well as developments in weapons technology. The journal aims to inform about procedures, background and trends in the aforementioned topics. The selection of publications is topic- and event-driven.

Disclosure according to §25 (1) Media Law (AUT)

Media owner is the TMW Horizont Gesellschaft mbH;
Tenschertstrasse 24/5/3, 1230 Wien

Editor-In-Chief: Matthias Wasinger, Ph.D.

Design: Lukas Bittner

Correspondence: contact@tdhj.org
ISBN: 978-3-200-10166-1

This special edition of The Defence Horizon Journal is produced in collaboration with The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) and comprises a synthesis of materials produced for the Cyber/Hybrid Symposium in April 2024 held by Hybrid CoE in Helsinki, Finland.

Hybrid CoE

THE DEFENCE HORIZON JOURNAL

Disclaimer

TDHJ Special Edition reflects the views of the authors, drawing on prior research and experience in their areas of expertise. The Defence Horizon Journal is a nonpartisan, independent Journal and does not take institutional positions.

Contents

DR TEIJA TIILIKAINEN

Director

The European Centre of Excellence for Countering Hybrid Threats

The geopolitical confrontation between democratic and authoritarian states is intensifying. New technologies are currently playing multiple roles in this conflict. As a key factor in states' economic resources, technological assets and capabilities have always played an important role in the global balance of power. Their role as a power resource has now multiplied due to the unlimited potential of disruptive modern technologies and the rapid pace of today's technology competition. Key differences in states' economic and political systems significantly affect the framework for this competition, with state-led economies increasingly distorting the global technology market's mechanisms.

Modern technologies, however, also play a key role in the geopolitical competition among great powers in which, apart from their global power position, their politico-military postures and resources are at stake. In this competition the revisionist powers seek to reorganize the international order to their own benefit by using all the tools at their disposal to strengthen their own position. Modern technologies thus also form a key tool in these battles in which democratic states' governmental structures, broad societal cohesion, and popular trust in democratic institutions and practices are targeted. This battle largely takes place in the cognitive and information domain, where an ability to affect structures of human thinking and the mental dimension becomes an important power resource. In this battle of cognitive superiority the unlimited potential of modern technology is deployed to steer and manipulate information, knowledge and discursive structures to the benefit of the actor in question. Cognitive superiority is also linked to an ability to maintain the superiority of a governance model and to decrease the competing model's legitimacy. In the current geopolitical confrontation this entails authoritarian regimes' ability to nourish disappointment and distrust in the democratic model and its possibilities of renewal and adjustment to changing societal conditions. It also means an ability to challenge the very foundations of the democratic model.

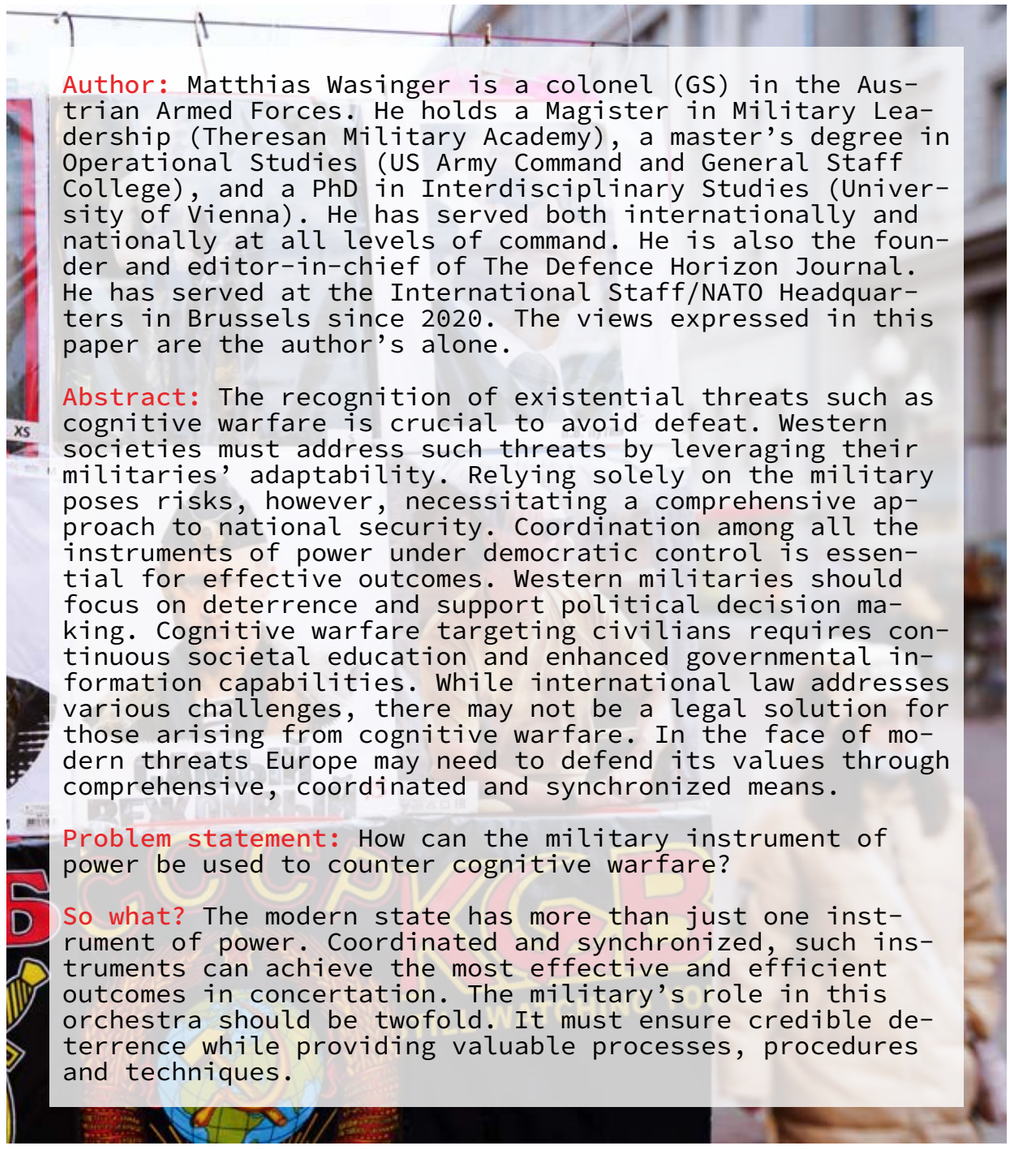
Along with the heightened geopolitical competition among states, technology and knowledge, which used to appear solid foundations of societal development, are increasingly becoming sources of insecurity and threats. Modern disruptive technologies amplify the risks of technology-dependent societies, the risks of interconnectedness of systems and failing resilience. Data security risks are multiplied due to capabilities related to quantum technologies and artificial intelligence. The triumph of modern technology is now increasingly becoming a dividing force between many types of winners and losers. The key beneficiaries of technological achievements will be further distanced from its downsides' victims. This divide becomes another force amplifying societal polarization and the lack of societal cohesion.

We have also already learnt to grasp the growing risks related to the modern use of knowledge and information to project power. The concept of strategic narratives refers to great powers' own understanding of their position on the global stage, how they reached it, and the direction in which they would like to take the international order. Their readings of the past are politicized to legitimize their desires for the future. Information about conflicts and their causes becomes highly subjective, which is nothing new, but this time modern technologies provide unlimited opportunities to spread these biased narratives, through which all events on the global stage tend to be interpreted. This leads to increasing waves of disinformation and other multiple efforts to dominate the battle of narratives. Reliable information sources are challenged and risk losing their credibility in the wider audience. There is no universal source of information with unassailable authority in the battle for facts and truth. Academic institutions must bend under the political pressure of authoritarian regimes.

It must be concluded that the current confrontation between democracies and autocracies is not only exceptionally deep but that it also targets the mental structures and complexities of the human mind much more effectively than ever. This creates huge challenges for democratic leaderships and all democratic societies to distinguish the externally driven manipulative forces from what can be seen as a purely domestic undercurrent of a democratic society. Many new tools and much expertise will need to be created to help tackle this challenge.

Then we will fight in the shade

MATTHIAS WASINGER



Author: Matthias Wasinger is a colonel (GS) in the Austrian Armed Forces. He holds a Magister in Military Leadership (Theresan Military Academy), a master's degree in Operational Studies (US Army Command and General Staff College), and a PhD in Interdisciplinary Studies (University of Vienna). He has served both internationally and nationally at all levels of command. He is also the founder and editor-in-chief of The Defence Horizon Journal. He has served at the International Staff/NATO Headquarters in Brussels since 2020. The views expressed in this paper are the author's alone.

Abstract: The recognition of existential threats such as cognitive warfare is crucial to avoid defeat. Western societies must address such threats by leveraging their militaries' adaptability. Relying solely on the military poses risks, however, necessitating a comprehensive approach to national security. Coordination among all the instruments of power under democratic control is essential for effective outcomes. Western militaries should focus on deterrence and support political decision making. Cognitive warfare targeting civilians requires continuous societal education and enhanced governmental information capabilities. While international law addresses various challenges, there may not be a legal solution for those arising from cognitive warfare. In the face of modern threats Europe may need to defend its values through comprehensive, coordinated and synchronized means.

Problem statement: How can the military instrument of power be used to counter cognitive warfare?

So what? The modern state has more than just one instrument of power. Coordinated and synchronized, such instruments can achieve the most effective and efficient outcomes in concertation. The military's role in this orchestra should be twofold. It must ensure credible deterrence while providing valuable processes, procedures and techniques.

Unfair game; two approaches

According to Herodotus, when threatened by the Persians with such a multitude of arrows that they obscured the sun during the Battle of Thermopylae in 480 BC, the Spartan warrior Dienekes responded, "Then we will fight in the shade".[1] In subsequent centuries several statesmen and philosophers have reattributed and reinterpreted this quotation. Its original meaning has evolved. The original statement underlined the paradoxically advantageous effect of fighting in the shade instead of under the blazing sun.[2] Another possible interpretation was added over the centuries, however: forbearance in clear sight of an overwhelming threat.[3] Confronted by an existential threat, ancient Greece, European culture's cradle, set the scene for winning a war by seeking an advantage in inferiority or defiant resistance.

More than two thousand years later, Europe again faces an existential threat. Russia's recent invasion of Ukraine is not a mere inter-state conflict at the continent's eastern edges. It is part of a campaign that seeks to eradicate the Western way of life, the recognized international legal framework, European values and supranational cohesion.[4] To this end, Russia and its partners have long waged a hybrid war against Europe. Unlike the Persian Wars, the weapons are no longer arrows. Disinformation campaigns, information warfare and cognitive warfare endanger social cohesion, transnational solidarity and public support for resistance to the external threat.[5] These means clearly fall below the threshold of armed conflict yet still challenge Western societies.[6] Once the threat is recognized and acknowledged, however, Europe may decide how to fight back by finding the advantage in turmoil or defiant forbearance.

No response without recognition

The cornerstone of any response to a threat is its official political recognition. As plain as this sounds, Europe especially still lacks situational awareness. Russia's military intrusions in Georgia in 2008 and Ukraine in 2014 were not followed by international condemnation or isolation.[7] On the contrary, a policy of appeasement and the deepening of economic dependence, especially on fossil energy, led to public ignorance of a painful fact: Russia's assertiveness was no longer limited to the diplomatic domain. Even the Russian government's blatant - and unfortunately successful - attempts to "hire" former high-ranking European politicians, including former German chancellor Gerhard Schröder and former French prime minister François Fillon, to gain an even deeper foothold in European political decision making were not taken seriously.[8] Even Russia's most recent invasion of Ukraine is still not recognized for what it is: a frontal attack on international law and order and European values.

The ongoing attritional warfare in Ukraine is just the most obvious symptom of Russia's aggression. Beneath this most cruel and visible campaign Russia and its partners are waging a more clandestine war against the West. It is a war for dominance in the information domain, a battle for superiority in attributing and interpreting information.[9] The aim is to shape how societies think about and influence the understanding of past, ongoing and future events and to diminish - if not annihilate - Western societies' trust and belief in values and their willingness to stand up for them.[10]

Although Western societies' support for Ukraine is remarkable and has undoubtedly enabled it to resist Russian aggression so far,[11] one might question whether the problem's entirety is recognized as a threat not only to a country on Europe's eastern edge but also as an attack on democratic concepts. Meanwhile, funds continue to flow to Ukraine, and weapon systems and ammunition are slowly but steadily being delivered to the East. Most European nations still lag in their energy independence, autonomous military deterrence and social

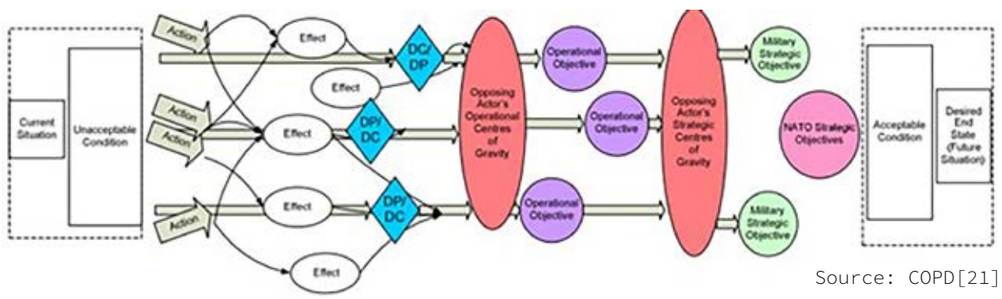
resilience targets.[12] It seems the superstition prevails that the current friction will be over one day, followed by a return to a new normal, with mutual trust, recognition of international law and good order.

Apparently, Russia's openly belligerent diplomatic, economic and even military threat posture has not (yet) crossed the threshold to be recognized for what it is - an existential threat.[13] Political statements outline the obvious. War does not begin with troop movements, economic blackmail, nuclear brinkmanship, cyberattacks, targeted killings, espionage and obvious human rights violations. It does not begin with strategic bombers and tanks crossing internationally recognized borders.[14,15] Both the People's Republic of China's "Unrestricted Warfare" and Russia's "Active Measures" clearly illustrate this.[16] Even if Western leaders wish to apply the legally institutionalized definition of war, these endeavours are in vain as long as one side decides no longer to acknowledge them. Clausewitz famously compared war with a wrestling match in which one side tried to compel the other to submit.[17] Cognitive warfare does exactly that. Peace needs the commitment of two sides; war only one. Wars start when political leaders recognize and declare (decide) that a war has started. As inconvenient as this decision appears, even with obvious belligerent deeds, it is more difficult to recognize clandestine acts below the threshold of conventional warfare as acts of war. Yet philosophy is the precursor of reality and the historical example: ignoring the multitude of incoming arrows may avoid a fight but not their deadly effect. The arrows are real, and they are aimed at the West.

Antagonist powers' attacks occur in the cognitive dimension. Cognitive warfare includes activities synchronized with other instruments of power to affect attitudes and behaviours by influencing, protecting or disrupting individual, group or population-level cognition to gain an advantage over an adversary. Whole-of-society manipulation has become a new norm designed to modify perceptions of reality, with the shaping of human cognition a critical warfare realm.[18] Given this definition, how can the military instrument of power counter or meaningfully support endeavours to counter such warfare? Defiant military forbearance or creativity in ambiguity? Waiting for a military escalation or comprehensive counteraction?

If all you have is a hammer, everything looks like a nail

The term cognitive warfare lends itself to an attribution to the military instrument of power. Ideally, states run a military to wage war or to respond to existential threats. Consequently, if cognitive warfare existentially threatens a state by attacking its social cohesion, delegitimizing its political leadership and even interfering in every democracy's highest good - elections - military means may be used to counter the threat. Cognitive warfare integrates cyber, information, psychological and social engineering capabilities,[19] all of which are available in the military.



Source: COPD[21]

To solve a problem, most Western militaries follow distinct planning steps. Political objectives are translated to military objectives. These objectives contribute to achieving a defined desired end state. (Decisive) conditions and effects, created by military and complementary non-military actions, define a roadmap for getting from an unacceptable to an acceptable condition.[20]

Whereas the collaborative planning process involves several levels of command, including institutional creativity and expertise, and the actual deeds on the ground, actions are (mainly) defined by those commands fighting in warfighting domains.[22] Although there is no commonly agreed definition of a warfighting domain, it can be defined as organizational constructs comprising an area of responsibility with a unique operational environment requiring distinct tactics, equipment and structure.[23] Likewise, NATO defines an operational domain as "a specified sphere of capabilities and activities that can be applied within an engagement space".[24]

Undoubtedly, cognitive warfare takes place in a (functional rather than geographical) area of responsibility within a unique operational environment, namely the human mind. Equipment and structures are derived from tasks and tactics. Yet these necessary tactics go beyond the doctrinal and indeed legal limitations of Western militaries. Western military doctrines explicitly exclude their populations from influence operations.[25] Besides, military efforts to shape how nations' populations think are clearly beyond Western societies' legal frameworks. Apparently, there is no cognitive warfighting domain;[26] and even if there were, Western militaries would be prohibited from operating in it against their own populations.

Moreover, for such an operational environment, military terminology appears too absolute, too Mahanian. Terms such as supremacy and superiority imply a kind of unchallenged dominance in respective dimensions. In an age of digitalization and connectivity information freely circulates online in accordance with European values. In this context cyberspace is both a means of transmission and a warfighting domain for disinformation, as well as information and cognitive warfare. Cyberspace has essentially facilitated the creation of the vitreous human and - potentially - transparent society. Digitalization and the everyday use of cyberspace have turned this artificial domain into a place of actual consequence, a diplomatic tool, an economic factor, a military effector and a social space satisfying the human need for social connectivity, for example. Cyberspace has contributed to the democritization of information while allowing malign actors to influence target audiences, set and dominate narratives, and exploit information.[27] No absolute supremacy in the cognitive dimension uses mainly democratized cyberspace.

The ongoing war in Ukraine has emphasized the dominance of a more Corbettian approach, meaning the necessity to achieve conditions that are good enough to make the best use of a certain (functional) area for a defined period.[28] This in turn seems achievable in both practical and legal terms, as the aim is neither social indoctrination nor permanent cognitive alignment. It remains questionable, however, whether the military is the most suitable instrument of power to do this.

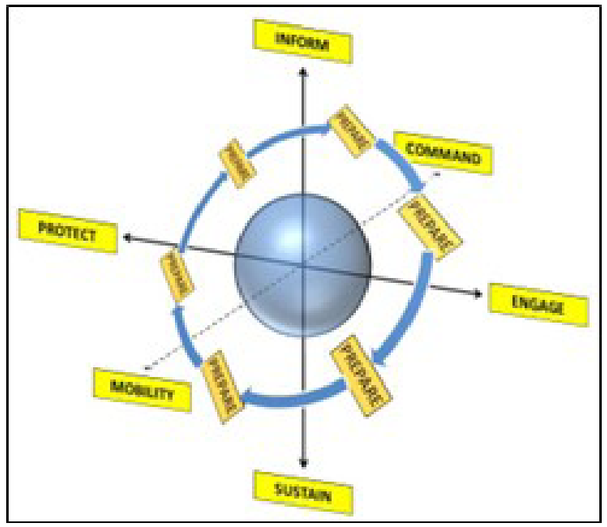
The military instrument of power is a nation's executive approach to external threats. This fact clearly distinguishes it from internally oriented police forces.[29] Tasking the military with either waging or countering cognitive warfare seems an obvious but futile choice. Although appropriate planning mechanisms are in place, neither a military's characteristics nor its democratically legitimized framework and organizational culture as a nation's existential guardian make it the right tool for the task. Cognitive warfighting brigades will not solve the problem. They would fight in the dark in de-

fiant forbearance, restricted, ill equipped, inappropriately trained and ultimately without achieving the desired effect.

Advantage in ambiguity

Cognitive warfare must be waged in synchronicity with other instruments of power to affect attitudes and behaviours. Military warfighting domains and dimensions such as cyberspace, the electromagnetic spectrum and the information realm are mere facets of a comprehensive concept. As such, the threats are not only a technical hack. They holistically harm our societies. They undermine democracies by diminishing both people's trust in politics and their willingness to defend our way of life. They challenge the legal and ethical framework by exploiting Western adherence to the rule of law and liberalism. (More or less) reasonable doubts, alternative truths and plausible deniability target human psychology in the information age. All these endeavours lead to geopolitical shifts that marginalize Europe's role on the world stage.[30] Holistic challenges call for comprehensive answers! The problem's solution therefore cannot be found in a single instrument of (hard) power.

Countering cognitive warfare and effectively responding to it if necessary (and appreciating its relevance for military planning and operations' execution) is mainly about preparation. All military capability areas - command, engage/operate, sustain, mobility/project, protect and inform - are based on proper preparation. Countering cognitive warfare in the "current" inevitably leads to a struggle for narrative dominance, the "absolute truth" and superior interpretation.[31] Unfortunately, Western societies have had to learn that "factual truth" as such does not matter. Once a narrative dominates the information realm, people's way of thinking is already shaped. Examples of this phenomenon range from the well-known (but non-existent) promise to Gorbachev concerning the inclusion of former Warsaw Pact states in NATO to Vladimir Putin's historical (but irrelevant and sometimes even absurd) claims on Ukraine.[32,33,34] Subjective truth - and only this matters to the individual - lies in people's beliefs. "Truth" lies in one's perception, and war happens when politicians say there is a war, not when tanks cross a border.



Source: Author

Russia has been at war with the West since Vladimir Putin stated this publicly on several occasions, among others during the 2008 Munich Security Conference.[35] It is a war that is still not actively waged with military means outside Ukraine. This should in turn mean that the West is at war too. Political leaders must face this inconvenience and accept it as fact. It is not a war the West chose to wage. It is a war that was imposed on the West, no matter how blatantly Vladimir Putin spins the facts. Western societies should therefore ensure both military deterrence and social resilience in all domains, dimensions and realms, and exploit strategic ambiguity. A society that is well informed about a state of war (especially one that is not waged by military means) is more willing to develop, support and contribute to deterrence and resilience.[36]

Indeed, a huge amount of work remains to be done in fields such as education (e.g. intellectual national defence, national security and defence policy, European values), governmental, semi-governmental and civil economy (strategic autonomy, national stockpiling), society (social cohesion, plurality, inclusivity and diversity management), and information technology (the value and curse of social media, digital literacy). Nevertheless, there is indeed a need for a military contribution. Militaries have developed processes and procedures throughout history that work in the worst imaginable circumstances and still deliver viable solutions.

Democracies have deficiencies in defining strategic objectives.[37] The military is capable of providing procedures to develop and frame achievable objectives.[38] A nation's sensors are so numerous, and the lines of communication so vast and complex, that achieving situational awareness is demanding. However, militaries have developed concepts to deal with complexity and complications.[39] Relations and connections between and within societies are multi-layered and shaped, among other factors, by history, culture and religion, so it is challenging to obtain and maintain a comprehensive understanding of social interaction.

Nevertheless, militaries have developed techniques to create, within means and capabilities, a comprehensive understanding of relevant actors, their interests, strengths, weaknesses and interconnections, even for out-of-area operations.[40] Through intrinsic need militaries have the ability to frame problems and define efficient approaches, structures, organizations and ultimately viable courses of action. Militaries possess the tools required to define effects and target audiences, assess risks and appropriate mitigating measures, and measure progress while advancing from an unacceptable to an acceptable status. They have all these tools and can provide them to decision makers, even without being the leading instrument of power.

This is not, of course, a call to reinvigorate militarism. Moreover, when emphasizing the need for political supremacy over the military instrument of power, Carl von Clausewitz explicitly mentioned the sovereign's need to appreciate the (military) experts' best advice.[41] When Clausewitz wrote On War, he did so from the perspective of a sovereign who controlled only one instrument of power, the military. We can assume that had they existed, he would have extended his theory to all other instruments of power.

Although a war may be waged with instruments other than the military, the military can offer support in response to non-kinetic/below-threshold threats such as cognitive threats. In doing so, it is indeed vital not to become a militaristic society. Besides military hard power, a crucial element of deterrence is maintaining and even expanding soft power - namely, European values, liberty and diversity.[42] There is nothing antagonist powers fear more than our open liberal democratic system.[43] Liberal democracy disqualifies the foundation of their power apparatus and ultimately delegitimizes their governance. Fighting in the shade allows the exploitation of strategic ambiguity. Necessary preparatory measures can be taken in the shade instead of under the blazing sun.

Fighting in the shade

To solve a problem, one must recognize that there is one in the first place. Ignoring it will inevitably lead to defeat. Once Western societies take that crucial step, political leaders must decide how to address these multidimensional existential threats: by finding the advantage in turmoil or defiant forbearance. Attributing the preparation

for any kind of warfare to the nation's warfighting instrument appears an obvious solution. Leaders should be aware of military adaptability and inherent obedience. This instrument of power will certainly take up the task and live up to it within its means and capabilities. Yet however adaptable we are, there is a risk that the hammer will treat the problem like a nail, especially given the (definitely required) legal restrictions. In forbearance the military would reactively fight with both hands tied behind its back in a dimension that asked for more comprehensiveness.

Fortunately, the modern state has more than just one instrument of power. Coordinated and synchronized, under the control of legitimized democratic leaders they can achieve the most effective and efficient outcomes in concertation. The military's role in this orchestra should be twofold. On the one hand it must deliver its raison d'être - namely, deterrence. On the other it can provide valuable processes, procedures and techniques to both the political leadership itself and other instruments of power.

Ultimately, one should bear in mind that cognitive warfare targets mainly civilians, the democratic sovereign. This is not a new phenomenon. About a hundred years ago, when elaborating on air power and military deep operations, Giulio Douhet wrote, "There will be no distinction any longer between soldiers and civilians. The defence on land and sea will no longer serve to protect the country behind them; nor can victory on land or sea protect the people…"[44] Humankind has found a solution to the problem in international law. This does not mean there will be a legal solution to the challenges imposed on the West by cognitive warfare. It is more likely that it will be an impetus to further educate societies or develop governmental information skills. One way or another it seems inevitable that Europe will again have to defend its existence and values by fighting in the shade.

Endnotes

[1] Herodotus, The Histories Book 7: Polymnia (Start Publishing LLC, 2015).

[2] Plutarch, Apophthegmata Laconica (Loeb Classical Library edition, Vol III, 1931).

[3] Valerius Maximus, Factorum et dictorum memorabilium, liber III.

[4] Peter Dickinson, 'Putin's Poisonous Anti-Western Ideology Relies Heavily on Projection', Atlantic Council, 3 July, 2022, accessed 7 March, 2024, https://www.atlanticcouncil.org/blogs/ukrainealert/putins-poisonous-anti-western-ideology-relies-heavily-on-projection/.

[5] Matthias Wasinger, 'The Highest Form of Freedom and the West's Best Weapons to Counter Cognitive Warfare', TDHJ.org, accessed 21 May, 2024, https://tdhj.org/blog/post/freedom-counter-cognitive-warfare/.

[6] Robert Seely, 'Defining Contemporary Russian Warfare', The RUSI Journal Volume 162, Issue 1 (2017): https://doi.org/10.1080/03071847.2017.1301634.

[7] Akaki Dvali, 'From Appeasement to Accountability - The West's New Approach Can Save Georgia from Putin', Newsweek, 19 March, 2024, accessed 11 May, 2024, https://www.newsweek.com/appeasement-accountability-wests-new-approach-can-save-georgia-putin-opinion-1880600.

[8] Hodun, Milosz and Cappelletti, Francesco, eds, Putin's Europe: Russia's Influence in European Democracy (ELF, 2023), 176-177.

[9] Geoffrey Roberts, '"Now or Never": The Immediate Origins of Putin's Preventative War on Ukraine', Journal of Military and Strategic Studies Volume 22, Issue 2 (2022).

[10] Ian Garner, 'The West Is Still Oblivious to Russia's Information War', Foreign Policy, 2024, accessed 11 May, 2024, https://foreignpolicy.com/2024/03/09/russia-putin-disinformation-propaganda-hybrid-war/.

[11] Congressional Research Service, Russia's War Against Ukraine: European Union Responses and U.S.-EU Relations (2024), https://crsreports.congress.gov/product/pdf/IN/IN11897.

[12] Council of the European Union, '"If We Want Peace, We Must Prepare for War"', news release, 19 March, 2024, accessed 11 May, 2024, https://www.consilium.europa.eu/en/press/press-releases/2024/03/19/if-we-want-peace-we-must-prepare-for-war/.

[13] Michael P. o. Liechtenstein, 'Is a Broader European War Imminent?', GIS, 2024, accessed 11 May, 2024, https://www.gisreportsonline.com/r/is-european-war-imminent/.

[14] Rosa Brooks, 'Can There Be War Without Soldiers?', Foreign Policy, 2016, accessed 11 May, 2024, https://foreignpolicy.com/2016/03/15/can-there-be-war-without-soldiers-weapons-cyberwarfare/.

[15] Seth G. Jones, Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare (New York, NY: W. W. Norton & Company, 2021), 73-76.

[16] Seth G. Jones, Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare (New York, NY: W. W. Norton & Company, 2021).

[17] Carl von Clausewitz, On War, ed. Michael Howard Princeton, NJ [u.a.]: Princeton Univ. Press, 1989, 75.

[18] Allied Command Transformation, Cognitive Warfare (2024), accessed 10 February, 2024, https://www.act.nato.int/activities/cognitive-warfare/.

[19] Idem.

[20] Allied Command Transformation, Comprehensive Operations Planning Directive: COPD INTERIM V2.0, 4-32 - 4-110.

[21] Ibid., 4-53.

[22] Ibid., 4-32 - 4-110.

[23] Everett C. Dolman, 'Space Is a Warfighting Domain', ÆTHER: A JOURNAL OF STRATEGY & AIRPOWER 1, Volume 1 (2022): 84, accessed 10 March, 2024, https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-1_Issue-1/11-Dolman.pdf.

[24] Allied Joint Publication-01, AJP-01 (NATO), no. 01, LEX-06.

[25] AJP-3.10, Allied Joint Doctrine for Information Operations (NATO), no. 3.10, 1-2 - 1-10.

[26] Patrick Hofstetter and Flurin Jossen, 'There Is No Need for a Cognitive Domain', TDHJ.org, 2 November, 2023, accessed 13 May 2024, https://tdhj.org/blog/post/no-need-cognitive-domain/.

[27] Matthias Wasinger, 'The Highest Form of Freedom and the West's Best Weapons to Counter Cognitive Warfare', TDHJ.org, accessed 21 May, 2024, https://tdhj.org/blog/post/freedom-counter-cognitive-warfare/.

[28] Julian S. Corbett, Some Principles of Maritime Strategy: A Theory of War on the High Seas; Naval Warfare and the Command of Fleets (Adansonia Press, 2018), 71-141.

[29] Matthias Wasinger, 'Vom Wesen und Wert des Militärischen: Interdisziplinäre Reflexion zum Alleinstellungsmerkmal des Militärischen zwischen Anspruch und Wirklichkeit' (Dissertation, Faculty of Law, 2017), 54-55.

[30] Matthias Wasinger, 'The Highest Form of Freedom and the West's Best Weapons to Counter Cognitive Warfare', TDHJ.org, accessed 21 May, 2024, https://tdhj.org/blog/post/freedom-counter-cognitive-warfare/.

[31] See for example: Government of Canada, 'Countering Disinformation with Facts - Russian Invasion of Ukraine', Government of Canada, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-fact-fait.aspx?lang=eng.

[32] Jeff Neal, '"There Was No Promise Not to Enlarge NATO" - Harvard Law School', Harvard Law School, accessed 14 May, 2024, https://hls.harvard.edu/today/there-was-no-promise-not-to-enlarge-nato/.

[33] NATO, 'NATO - Official Text: Founding Act on Mutual Relations, Cooperation and Security Between NATO and the Russian Federation Signed in Paris, France, 27 May 1997', accessed 13 May 2024, https://www.nato.int/cps/su/natohq/official_texts_25468.htm.

[34] Government of Canada, 'Countering Disinformation with Facts - Russian Invasion of Ukraine', Government of Canada, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-fact-fait.aspx?lang=eng.

[35] Nick Fishwick, 'Putin Has Declared War on the West. It's Time to Take the Fight to Russia', The Cipher Brief, 19 February, 2024, accessed 9 May, 2024, https://www.thecipherbrief.com/column_article/putin-has-declared-war-on-the-west-its-time-to-take-the-fight-to-russia.

[36] Michal Onderco, Wolfgang Wagner, and Alexander Sorg, WHO ARE WILLING to FIGHT for THEIR COUNTRY, and WHY? (2024), accessed 7 May, 2024, https://spectator.clingendael.org/en/publication/who-are-willing-fight-their-country-and-why.

[37] Donald J. Stoker, Why America Loses Wars: Limited War and US Strategy from the Korean War to the Present, Revised and updated [edition] (Cambridge: Cambridge University Press, 2022), 53-60.

[38] Allied Command Transformation, Comprehensive Operations Planning Directive: COPD INTERIM V2.0, 3-19 - 3-36.

[39] NATO Science and Technology Organization, 'Visualisation and the Common Operational Picture', accessed 13 May, 2024.

[40] Allied Command Transformation, Comprehensive Operations Planning Directive: COPD INTERIM V2.0, 4-13 - 4-48.

[41] Carl von Clausewitz, On War, ed. Michael Howard, (Princeton, NJ [u.a.]: Princeton Univ. Press, 1989), 608-609.

[42] Robert Service, The Penguin History of Modern Russia: From Tsarism to the Twenty-First Century, 4th ed. (London, UK: Penguin, 2021), 571-591.

[43] Timothy Frye, Weak Strongman: The Limits of Power in Putin's Russia (Princeton and Oxford: Princeton University Press, 2021), 12-14.

[44] Giulio Douhet, The Command of the Air, USAF warrior studies Washington, D.C.: Air Force History and Museums Program, 1942, 10.

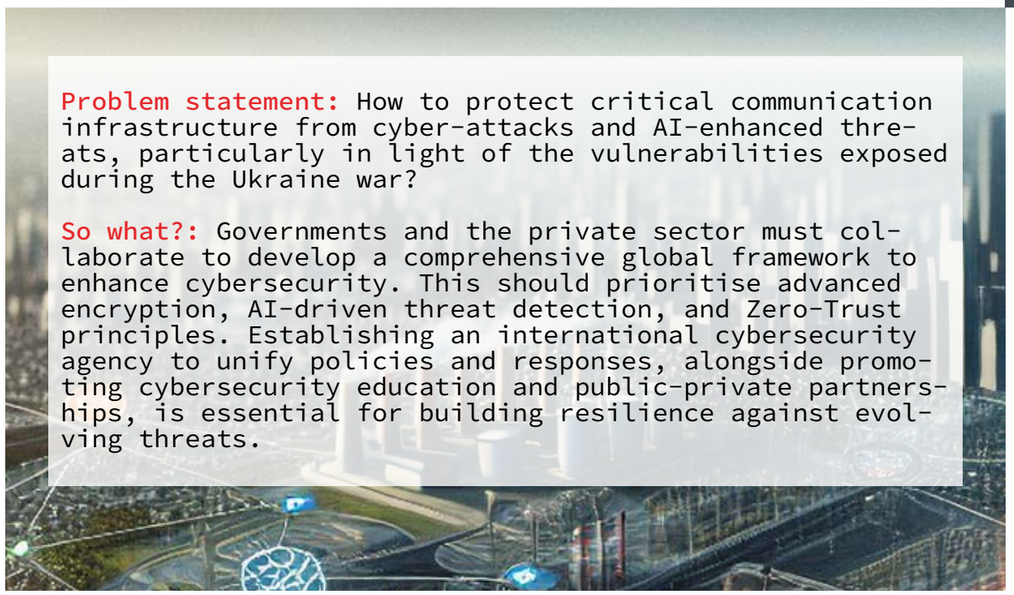
Legal And Strategic Approaches

To AI-Enhanced Threats In Critical Infrastructure

BIANCA LINS

Author: Dr. Bianca Lins, LL.M.; Space, Cybersecurity, Critical Infrastructures, Electronic Communications, AI, Law; publications include i.a. Lins/Schroefl (Hrsg). The Cyber and Information Space Matrix: A Conceptual Framework, including Critical Infrastructure Space (to come); Lins. Guiding & Inspiring the Next Generation of Cybersecurity Professionals. DigitalFirst Magazine, 2/2024; Lins. Space Diplomacy. Top Cyber News Magazine, June 2024; Lins. Cybersecurity in M&A Transactions within the Satellite Industry. Top Cyber News Magazine, June 2024; Cybersicherheit von Kryptoassets. In Piska/Völkel (Hrsg), Blockchain Rules2 (2024). Wien: Manz; Lins. Internationales Weltraumrecht und die Rolle des nationalen (Liechtensteinischen) Rechts: Eine Einführung. LJZ - Liechtensteinische Juristen-Zeitung, 3/2023; Law, Space, Cybersecurity. The views contained in this article are the author‘s alone and do not represent the views of the Liechtenstein Administration.

Abstract: In today‘s interconnected world, communication networks form the backbone of society, enabling global connectivity and innovation. However, these systems are vulnerable to cyber-attacks, as evidenced by Russian forces targeting satellite-based networks during the Ukraine war, disrupting crucial services. This highlights the need to protect critical infrastructure from digital threats. AI-enhanced threats exacerbate vulnerabilities but also offer defence opportunities. To fortify against disruptions, strengthening legal frameworks, fostering international cooperation, and leveraging AI for defence is essential. Addressing these challenges requires a multifaceted international approach to safeguard our critical digital infrastructure from evolving cyber threats.



Problem statement: How to protect critical communication infrastructure from cyber-attacks and AI-enhanced threats, particularly in light of the vulnerabilities exposed during the Ukraine war?

So what?: Governments and the private sector must collaborate to develop a comprehensive global framework to enhance cybersecurity. This should prioritise advanced encryption, AI-driven threat detection, and Zero-Trust principles. Establishing an international cybersecurity agency to unify policies and responses, alongside promoting cybersecurity education and public-private partnerships, is essential for building resilience against evolving threats.

Fragile Connectivity Faces Growing Cyber Threats

In today's increasingly interconnected world, the fabric of our daily lives is woven with intricate and often invisible communication threads. These threads encompass various technologies, from telecommunication networks to satellite connections, forming the essential infrastructure that supports our modern society. This critical framework facilitates global connectivity and drives continuous innovation, acting as the backbone of our daily operations and interactions.

However, much like a delicate spider's web, this infrastructure is inherently fragile and susceptible to various threats. While physical threats have traditionally been considered the primary danger, the digital age has introduced a new and pervasive menace: cyber-attacks. As the global dependence on technology grows, so does the risk of cyber-attacks targeting these vital systems. These attacks, executed through the realm of bits and bytes, can potentially disrupt, damage, and dismantle the very networks on which societies worldwide rely.

In the context of the ongoing war in Ukraine, Russian forces have strategically targeted communication networks dependent on satellite technology. A prominent example occurred at the very onset of Russia's invasion when a cyberattack was launched against ViaSat's KA-SAT satellite network.[1] This attack not only resulted in a significant loss of communications for the Ukrainian military but also had widespread ramifications across Europe. Thousands of users were affected, including 5,800 German wind turbines that were rendered offline for weeks, illustrating the extent of collateral damage caused by such cyberattacks.[2]

The Russian invasion and its accompanying cyber warfare have underscored the critical necessity of protecting global infrastructure. A successful breach of critical infrastructure can have catastrophic consequences, impacting economic stability, public safety, and national security. The ViaSat attack exemplifies how vulnerable interconnected systems are and how essential services can be disrupted, highlighting the fragile nature of our technological dependencies.

The technology landscape continues to evolve rapidly. One of the most pressing concerns is the emergence of AI-enhanced threats, which have shown a marked increase in sophistication. These advanced cyber threats pose new challenges to global efforts in securing critical infrastructure, making it imperative to stay ahead of potential vulnerabilities.

Cutting-Edge Technologies, Robust Policy Frameworks & International Cooperation

This evolving threat landscape necessitates a proactive approach to cybersecurity that involves adopting cutting-edge technologies, robust policy frameworks, and international cooperation. By understanding the intricate dynamics of cyber warfare and investing in resilient infrastructure, governments, industries, and global stakeholders can better prepare to defend against these sophisticated attacks, ensuring the stability and security of our global communication networks.

Over the past 25 years, the communications industry has undergone a profound transformation, evolving into a complex network that integrates terrestrial, satellite, and wireless systems. These components are intricately interconnected, creating a multifaceted and dynamic sector. Initially focused primarily on providing voice services, the industry has expanded into a highly competitive and integrated field, offering diverse services. This interconnectedness means that providers across various platforms-satellite, wireless, and wireline-rely on each other to sustain and complete their traffic, often sharing facilities and technologies to ensure seamless interoperability.

The ownership and operation of most of this communications infrastructure lie within the private sector. Consequently, it is primarily the private sector's responsibility to ensure the protection and security of its infrastructure and assets. However, the complexity and interdependence of modern communication networks necessitate robust collaboration with governments. Public-private partnerships are crucial in predicting, anticipating, and responding to cyber threats. Such cooperative efforts are essential for safeguarding the integrity of communications, especially during critical times. Maintaining these partnerships is vital for the immediate functioning of communication networks and understanding and mitigating the broader implications of potential disruptions. Effective collaboration ensures that national leadership can communicate during emergencies, supports the operations of other critical sectors, and enhances the overall effectiveness of response and recovery initiatives. In an era where the technology landscape is continuously evolving, the combined efforts of both the private and public sectors are indispensable for maintaining the resilience and security of our communication infrastructure.

The Vital Role of Communication Networks

Today, the communications sector underpins the functionality of diverse industries, making it an indispensable pillar of modern infrastructure. This interdependence highlights the critical nature of robust and secure communication networks across various domains.[3] One prime example is the relationship between the communications and energy sectors. The energy sector supplies the power to operate cellular towers and communication facilities. Conversely, it relies on robust communication systems to efficiently monitor and control electricity delivery. Communication networks enable real-time data transmission, which is crucial for maintaining the stability and reliability of power grids and managing energy resources effectively.

Similarly, the information technology (IT) sector heavily depends on communication networks, which form the backbone of critical control systems, physical architecture, and internet infrastructure. These networks are essential for distributing applications and services, ensuring data flows seamlessly across platforms and devices. The synergy between IT and communications is vital for supporting various digital operations and innovations that drive economic growth and societal advancement.

The financial services sector also relies on secure and reliable communication networks to execute transactions and manage the operations of financial markets. The integrity and confidentiality of financial data depend on robust communication infrastructures to prevent fraud and ensure the smooth functioning of global financial systems. Secure communications are indispensable for maintaining trust and stability within the financial ecosystem.

In the realm of public safety, the emergency services sector utilises communication technologies for resource coordination, emergency responses, public alerts, and handling emergency calls. Effective communication is the cornerstone of efficient emergency management, enabling quick and coordinated responses to crises, thereby saving lives and mitigating damage. The transportation systems sector depends on communication systems to oversee and manage traffic movement across ground, sea, and air routes. Communication networks facilitate the real-time exchange of information necessary for navigation, traffic control, and logistics management, ensuring the safe and efficient transport of goods and passengers.

These examples underscore robust communications systems' importance as a critical infrastructure cornerstone. Given this significance, it is clear that communications systems remain a prime target for nation-state threat actors. These adversaries are increasingly leveraging the power of artificial intelligence (AI) to employ more sophisticated and stealthy techniques. AI-enhanced methods allow these actors to establish long-term presence and evade detection more effectively, posing significant challenges to cybersecurity. By harnessing AI, threat actors can automate complex tasks, refine their strategies, and adapt quickly to changing security environments. This makes it increasingly difficult to protect vital systems against breaches and disruptions. The dual-use nature of certain infrastructures, such as space-based communication systems, which serve both civilian and military purposes, further amplifies the risk. Protecting these systems is paramount to ensuring national security, economic stability, and public safety.

The Responsibility of Safeguarding Critical Infrastructure

Yet, the primary responsibility for safeguarding the infrastructure and assets of the communications sector lies with the private sector. Envision the catastrophic impact if communication systems were to fail for a day, a week, or even a month. Such failures would disrupt technical operations and have profound ripple effects across geopolitical, social, economic, and psychological domains. The economy would suffer, societal functions would be hindered, national security would be compromised, and the psychological well-being of the population would be severely affected.

Since Russia's most recent invasion of Ukraine, the global cyber threat landscape has dramatically evolved.[4] More aggressive state actors now engage in hybrid warfare, blending traditional military tactics with sophisticated cyber operations.[5] The ViaSat hack is a clear example of how cyber operations extend beyond the immediate conflict in Ukraine, impacting a wide range of targets. The cyber battlefield now includes social media platforms, private and public information networks,

and critical infrastructures. Western companies, media, and government services are increasingly being attacked, with AI being utilised in various forms to enhance the sophistication and effectiveness of these assaults.[6]

These hybrid threats pose a severe risk of escalating conflicts and increasing the likelihood of direct confrontations between nations. Despite the growing urgency, achieving effective cooperation among democratic governments, agencies, and the private sector in the realm of cybersecurity remains a significant challenge.

Governments worldwide are indeed taking steps to enhance the security and resilience of critical infrastructure through various regulations.[7] These efforts are crucial in bolstering cyber defences. However, the introduction of new laws and regulations also brings challenges, such as the potential for overlapping or inconsistent requirements across different jurisdictions, which can complicate compliance and implementation.[8] To effectively combat cyber threats, a broader, multifaceted approach is essential. This approach should include updating and harmonising legal frameworks across jurisdictions to close regulatory gaps and ensure consistent enforcement of cybersecurity standards globally. Fostering international collaboration is critical - this requires coordinated efforts between governments, international organisations, and the private sector to share intelligence, establish common protocols, and respond swiftly to cyber incidents. Involvement from industries is equally important, as they are often the first line of defence against cyberattacks. Furthermore, harnessing the potential of AI for defence involves investing in AI-driven threat detection systems, automating responses to cyber incidents, and developing machine learning algorithms that can adapt to emerging threats in real-time. By integrating these elements, such a strategy will not only fortify critical infrastructure but also anticipate and mitigate future cyber threats in a rapidly evolving technological landscape.

Shifting the cybersecurity posture from one of reaction to one of proactive, cooperative, and holistic defence is essential. This involves anticipating threats before they manifest, fostering information sharing across borders and industries, and developing adaptive strategies leveraging technological advancements. For instance, AI and machine learning are increasingly being used to detect threats in real-time by analysing vast amounts of data for unusual patterns of behaviour, as seen in platforms like Darktrace and CrowdStrike. These technologies enable faster detection and response to cyberattacks. Additionally, automated incident response systems, such as SOAR (Security Orchestration, Automation, and Response), allow for the automation of responses to detected threats, improving response times and reducing human error. By implementing such measures, vital systems can be better protected, ensuring their resilience and maintaining the continued stability of an increasingly interconnected world.

A Global Cooperative Cybersecurity Framework

Developing a comprehensive global cybersecurity framework that encompasses strategic, legal, and technical aspects is imperative to address the ever-evolving landscape of cyber threats. This framework must be designed to ensure robust cybersecurity measures while promoting international cooperation and the adoption of advanced technologies.

Firstly, the framework should implement robust cybersecurity measures and include comprehensive updates and enforcement of international laws. This involves establishing common grounds on the application of international law and clarifying how it applies to the behaviours of different actors in cyberspace. By creating a unified legal approach, nations can better coordinate their efforts to deter and respond to cyber threats.

Moreover, the legal regulations within this framework must facilitate international cooperation and interoperability across various sectors. Encouraging the adoption of advanced technologies is crucial to staying ahead of cyber adversaries. Legal measures should focus on not only addressing immediate vulnerabilities but also promoting an environment of continuous improvement and learning. This includes laying the groundwork for enhanced encryption, authentication, biometrics, analytics, and automated network security.

Public-private cooperation must be a cornerstone of this framework. Enhanced collaboration regarding cyber threat intelligence sharing is essential. Protecting critical technologies, such as cloud computing and data centres, requires a joint effort between governments and the private sector. Legal regulations should foster such cooperation, ensuring that both parties are equipped to share information and resources effectively.

Resiliency must also be a key focus. This can be achieved through targeted investments, partnerships, and international cooperation. Enhancing the resilience of critical infrastructures allows for better preparation to withstand and recover from cyber-attacks. Laws should support these efforts by encouraging investments in cybersecurity measures and promoting collaboration between nations and industries.

Another critical component is improving the investigation and prosecution of cybercrimes, particularly ransomware attacks and targeting illicit cryptocurrency exchanges. Effective legal frameworks should equip law enforcement agencies with the necessary tools and resources to track, apprehend, and prosecute cybercriminals. This includes enhancing cross-border cooperation and establishing clear protocols for investigating cybercrimes.

In addition, a concerted effort must foster an environment of innovation and technological advancement within cybersecurity. This involves investing in cutting-edge research and development and ensuring that there are pathways for the swift adoption and implementation of new technologies. Educational initiatives and training programs are essential to cultivate a skilled workforce in the latest cybersecurity techniques and methodologies.

Another important aspect is the establishment of global standards and best practices. Organisations and nations can ensure a cohesive and unified defence against cyber threats by developing and adhering to universally accepted cybersecurity protocols. These standards should be continuously reviewed and updated to reflect the latest technological advancements and emerging threats.[9]

Finally, promoting a culture of cybersecurity awareness and responsibility at all levels of society is crucial. Public awareness campaigns, industry-led initiatives, and governmental policies should all aim to educate individuals and organisations about cybersecurity's importance and their role in maintaining a secure digital environment.

A Coordinated and Multifaceted Approach

Developing this comprehensive global cybersecurity framework is not only necessary but urgent. The complexity and scale of cyber threats require a coordinated and multifaceted approach that leverages the strengths of all stakeholders involved. Through strategic, legal, and technical collaboration, a robust defence system can be built to protect critical infrastructure and ensure the stability and security of an interconnected world.

To build an effective global cooperative cybersecurity framework, it is essential to establish clear priorities that address the multifaceted nature of cyber threats and the

diverse needs of the stakeholders involved. These priorities should encompass a range of strategic, technological, and collaborative efforts to enhance global cybersecurity resilience.

A priority should be identifying and continuously monitoring the evolving threat landscape posed by state actors and advanced criminal hacking groups. Understanding these adversaries' tactics, techniques, and procedures is crucial for developing proactive defence mechanisms. This requires a robust intelligence-gathering infrastructure, supported by international collaboration, to share insights and threat intelligence in real-time.

Securing critical infrastructure through the adoption of new technologies is another vital aspect. This includes the modernisation of security architectures and the adaptation of strategies based on security by design principles. By integrating security measures at the inception of system development rather than as an afterthought, inherently secure infrastructures can be created, making them more resistant to attacks.

Advanced encryption and biometric technologies should also be a focal point. Developing quantum-proof encryption methods and keyless authentication systems will be essential in safeguarding sensitive data against future threats posed by advancements in quantum computing. These technologies will provide robust protection for communication channels and critical data repositories.[10]

The further development and deployment of AI technologies are crucial for real-time horizon scanning and network monitoring. AI can significantly enhance our ability to detect and respond to emerging threats by analysing vast data at unprecedented speeds. This will enable more effective threat detection, rapid response, and mitigation strategies.[11]

Access and identity management, aligned with Zero-Trust guidelines, should be prioritised to ensure that only authenticated and authorised users can access critical systems and data. Implementing strict access controls and continuous verification processes will minimise the risk of unauthorised access and potential breaches.

Endpoint protection must also be addressed, particularly in the context of the Internet of Things (IoT) and hardware security vulnerabilities. IoT refers to the vast network of interconnected devices - ranging from smart home appliances to industrial sensors - that communicate and exchange data via the internet. These devices often lack robust built-in security, leaving them susceptible to cyberattacks. Securing these endpoints has become increasingly complex with the proliferation of connected devices. Employing comprehensive endpoint protection strategies will help safeguard against threats targeting these devices and the networks they connect to.

Cooperative cyber-incident response mechanisms are essential for effectively managing and mitigating the impact of cyber incidents. Establishing protocols for coordinated responses across borders and sectors will enhance our ability to contain and resolve incidents swiftly, minimising damage and facilitating recovery.

Fragmentation of Current Efforts

While numerous initiatives and collaborations are already making significant progress, the need for a more strategic and cohesive approach remains evident. The fragmented nature of current efforts often leads to inefficiencies and gaps in our collective cybersecurity defences. It is imperative to consider adopting a more centralised approach to address the growing cybersecurity threats and the limitations posed by our existing cybersecurity strategies and governance structures. While achieving consensus on such a framework at the United Nations level may be challenging due to varying member state interests, and NATO and the EU do not encompass all nations, bringing together stakeholders from governments, academia, industry, and international organisations is crucial. This diverse coalition can help coordinate efforts without imposing unwanted oversight, respecting participating entities' sovereignty and operational independence. Therefore, a compelling proposal is the establishment of an international agency that transcends the boundaries of existing transnational organisations and supranational structures such as the European Union, the G-7, and NATO.

This approach requires fostering a spirit of collaboration where stakeholders voluntarily share information, best practices, and resources. Establishing forums and platforms for regular dialogue and cooperation will facilitate this process, ensuring that all parties remain engaged and committed to the collective goal of enhancing global cybersecurity resilience.

A centralised international agency would serve as a focal point for global cybersecurity efforts, facilitating deeper international cooperation among Western allies. This enhanced collaboration is pivotal in addressing the complexities of modern cyber threats, which often transcend national borders and require a coordinated response. Such an agency could harmonise policies, standardise best practices, and ensure a rapid, unified response to emerging threats. Furthermore, this proposed approach would enhance the protection of critical infrastructures and bolster societal resilience and national security. A more robust defence mechanism could be created by fostering a deeper level of cooperation among like-minded Western allies, leveraging participating nations' collective strengths and resources. This would enable a more comprehensive understanding of the cyber threat landscape, as the international agency could provide a clearer picture of adversaries' tactics, techniques, and procedures by pooling intelligence and resources. This collective intelligence would be invaluable in developing proactive defence strategies and staying ahead of evolving threats.

The centralised agency could also play a crucial role in advancing research and development in cybersecurity. By coordinating efforts across nations and industries, innovation and the adoption of cutting-edge technologies could be driven forward, enhancing current defences and preparing for future challenges, ensuring resilience in the face of rapidly evolving cyber threats.

Additionally, the agency would facilitate improved incident response and crisis management. A centralised entity responsible for coordinating responses to cyber incidents can ensure a more efficient and effective reaction to major breaches and attacks. This would involve technical mitigation and strategic communication and recovery efforts, minimising the impact on affected sectors and populations.

A Global Cybersecurity Framework

The necessity for a comprehensive global cybersecurity framework has become increasingly evident in today's interconnected and technology-dependent world. The vulnerabilities exposed by recent cyberattacks, such as those on ViaSat's KA-SAT satellite network during the ongoing conflict in Ukraine, underscore the critical need for robust and coordinated cybersecurity measures. These incidents have highlighted the fragility of communication networks and the profound ripple effects that disruptions can cause across geopolitical, social, economic, and psychological domains.

The transformation of the communications industry over the past 25 years into a complex, interconnected network of terrestrial, satellite, and wireless systems further amplifies the importance of securing these infrastructures. The private sector, which owns and operates most of this infrastructure, bears significant

responsibility for its protection. However, the complexity and scale of modern cyber threats necessitate a collaborative approach involving both the private sector and governments.

The proposed global cybersecurity framework should prioritise identifying and monitoring evolving threats, securing critical infrastructure with new technologies, and modernising security architectures. Emphasis should be placed on advanced encryption, biometric authentication, AI-driven threat detection, and adherence to Zero-Trust principles in access and identity management. Additionally, comprehensive endpoint protection and cooperative cyber-incident response mechanisms are essential to address the vulnerabilities associated with the IoT and other emerging technologies.

Public-private cooperation is crucial for effective cybersecurity. Enhanced collaboration on threat intelligence sharing, protection of critical technologies, and investments in resiliency measures will strengthen collective defences. Legal frameworks must evolve to facilitate international cooperation, promote continuous improvement, and support the adoption of advanced security measures.

The establishment of a centralised international agency dedicated to cybersecurity, transcending existing structures such as the European Union, G-7, and NATO, would provide a strategic, unified approach to managing cyber threats. This agency would harmonise policies, standardise best practices, and coordinate responses to cyber incidents, leveraging the collective strengths and resources of participating nations and industries.

Moreover, fostering a culture of cybersecurity awareness through educational initiatives and training programs is essential. Equipping professionals with the necessary skills and promoting a collective sense of responsibility will contribute to a more resilient cybersecurity posture.

The path forward requires a multifaceted and proactive approach. By integrating strategic, legal, and technical elements into a cohesive global framework - and allowing room for tailored national responses - international cooperation and innovation can flourish. This will help protect critical infrastructures and ensure the stability and security of the digital world. Such an approach will enable the anticipation and mitigation of cyber threats effectively, safeguarding societies and economies against the challenges of the evolving cyber landscape.

Endnotes

[1] "KA-SAT Network cyber attack overview," Viasat Inc., March 30, 2022, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

[2] “The war in Ukraine from a space cybersecurity perspective,” European Space Policy Institute (ESPI) (October 2022): 6.

[3] Soledad Antelada Toledano, Critical Infrastructure Security - Cybersecurity Lessons Learned from Real-world Breaches (Birmingham: Packt Publishing, 2024), 3-31.

[4] Itzhak Aviv/Uri Ferri, "Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem," International Journal of Critical Infrastructure Protection, Volume 43, (December 2023): 100637.

[5] "Russia's hybrid war against the West," NATO Review, Arsalan Bilal, April 26, 2024, https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html; "New Threats, Complexity, and 'Trust' as the Antidote," NATO Review, Arsalan Bilal, November 30, 2021,

https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

[6] "International Community Must Urgently Confront New Reality of Generative, Artificial Intelligence, Speakers Stress as Security Council Debates Risks, Rewards," United Nations SC/15359, July 18, 2023, https://press.un.org/en/2023/sc15359.doc.htm; "Journalists & Cyber Threats," Center for News, Technology & Innovation, July 23, 2024, https://innovating.news/article/journalists-cyber-threats/; "Beware of AI-enhanced Cyberattacks," Emily Otto, January 30, 2024, https://cepa.org/article/beware-of-ai-enhanced-cyberattacks/; Nusrat Kabir Samia, "Global Cyber Attack Forecast using AI Techniques," Electronic Thesis and Dissertation Repository, (August 2023): 9582; "AI in Cyber Warfare: AI-Powered Attacks and Defense," George Dobrea, July 09, 2024, https://www.eccouncil.org/cybersecurity-exchange/cyber-talks/ai-in-cyber-warfare/.

[7] "Cybersecurity laws and legislation (2024 update)," Connectwise, Michael Brands, June 05, 2024,

https://www.connectwise.com/blog/cybersecurity/cybersecurity-laws-and-legislation.

[8] European Commission, “Commission Staff Working Document Impact Assessment Report,” SWD(2020) 345 final, Part 2/3, December 16, 2020, 101; “Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information,” Office of the National Cyber Director, The White House, (June 2024): 10.

[9] An example of responding to emerging technological developments is NIST's release of the first finalised post-quantum encryption standards in August 2024, aimed at protecting systems from quantum computing threats. Similarly, ENISA is actively refining governance frameworks to implement national cybersecurity strategies, ensuring they adapt to new challenges; https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards; https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools.

[10] Chandrababu Kuraku/Shravan Kumar Rajaram/Hemanth Kumar Gollangi/Venkata Nagesh Boddapati/ Gagan Kumar Patra, "Advanced Encryption Techniques in Biometric Payment Systems: A Big Data and AI Perspective," Library Progress International Volume 44 No. 3, (Jul-Dec 2024): 2447-2458; "Discover the latest in cutting-edge biometric technology for the future," Veriff, Geo Jolly, August 28, 2024, https://www.veriff.com/identity-verification/news/the-future-of-biometric-technology.

[11] Maruf A. Tamal/Md K. Islam/Touhid Bhuiyan/Abdus Sattar/Nayem Uddin Prince, "Unveiling suspicious phishing attacks: enhancing detection with an optimal feature vectorisation algorithm and supervised machine learning," Frontiers in Computer Science, (July 2, 2024): 6; Rakibul Hasan Chowdhury/Nayem Uddin Prince/Salman Mohammad Abdullah/ Labonno Akter Mim, "The role of predictive analytics in cybersecurity: Detecting and preventing threats," World Journal of Advanced Research and Reviews, (July 2024), 23(02), 1615-1623.

From Hunches To Forecasts – Combining Machine And Human Intelligence For Cyber-Information Sense-Making

CHRIS BRONK

Author: Chris Bronk, Ph.D., is an associate professor at the University of Houston's Hobby School of Public Affairs. He studies the intersection of information and computing technology with international relations. The views contained in this article are the author's alone and do not represent the views of the University of Houston nor the State of Texas.

Abstract: Hybrid warfare operations embrace "anything that gets results" strategy, including significant information operations. Western democracies need to better understand the information operations that are undertaken against them. This will need to involve more rigorous observation, monitoring, and measurement of malign political campaigns undertaken against them via the Internet.

Problem statement: How can hybrid information influence conflict operations be detected, tracked, and countered?

So what?: The most open societies are likely the most vulnerable to data manipulation and information operations. The community of democratic states must erect defences against malign information influence delivered through cyberspace.

A Transformation in Information Power

More than eighty years ago, British diplomat, journalist and academic Edward Hallett Carr declared in his The Thirty Years Crisis that power could be exerted in three areas - military, economic, and information.[1] Substituting his term soft power for power over opinion, Nye produced a similar assessment six decades later.[2] While agreement may exist between practitioners and scholars that information power is important, borrowing from Simon, one must ask, "to what extent have the operational tools of observation and measurement been provided us?"[3] The task at hand for scholars and practitioners of the geopolitical information environment is to identify how burgeoning sources of information may be processed and analysed by novel computational methods referred to as artificial intelligence (AI).

What Makes for Information Awareness in Hybrid Conflict?

Resilient, accurate situational awareness of hybrid threats depends on observation and measurement in each sub-area in the hybrid arena, which blends "the lethality of state conflict with the fanatical and protracted fervour of irregular warfare."[4] Such observation translates to monitoring many different types of activity undertaken by an adversary. Governments and other actors have created all manner of observation and measurement capacities, from social media and banking systems to computer networks and reconnaissance satellites. How this new form of interstate conflict is set apart from our fading memories of the Cold War is that where once data was hard to find, now there is often an overabundance of it.[5] However, new issues arise. Data of sufficient quality may be used to measure phenomena, and that measurement is a key step to situational awareness.[6]

Computing has given humankind a greater capacity to assign quantitative measures to all manner of phenomena. Mobile computing devices provide sensor data from images to geolocation.[7] At the outset of the February 2022 invasion of Ukraine, images of military action, largely taken from mobile devices, flooded social media.[8] Open-source intelligence (OSINT) analysts, mostly amateurs, sifted through online video and images of combat to generate a picture of the military action.[9]

As for combining inputs at a strategic level and then translating them to operational action, the most important issues will be the accuracy of the information inputs from all sources and the timeliness of their analysis. An example of success in this area is the Ukrainian missile attack on the port at Berdiansk in March 2022.[10] Russia released a propaganda video of its operations at the seaport, which allowed accurate Ukrainian targeting of Russian amphibious ships there. The Ukrainian missile attack then sank one of the ships and badly damaged two others.[11] This form of OSINT may be highly useful; however, incorporating it into a rapid, task-oriented intelligence analysis enterprise holds challenges, not least the potential for disinformation by a wary enemy.

The intelligence picture available to government, industry, and individuals today is very different from what it was during the last period of major power competition, which ended with the demise of the Soviet Union.[12] The enormous technological advances in information and computing technologies (ICTs) have completely overhauled the craft of intelligence. Foreign agents can be recruited in chat rooms rather than back alleys. Overhead intelligence, which was the province of superpowers, is now available commercially by download over the Internet. There's no need to break open file cabinets when computers may be electronically compromised, and contents pilfered by actors half a world away. For the collectors of intelligence, a bonanza of sorts exists. However, for those being collected from, an acknowledgement of the huge value of their "digital

exhaust”[13] comes only after that data is translated into action—from online censorship to artillery bombardment. The communications revolution represents a double-edged sword for high-technology societies and their high-technology militaries.

There is no question that mobile smartphones, which perform the role of everything from calculators and cameras to media studios and flashlights, have made an enormous impact on humanity.[14] The number of cellphone subscriptions surpassed the global population sometime between 2015 and 2020.[15] Sweden’s Ericsson, the builder of the technological infrastructure that runs mobile communication, contends that some 60 per cent of the planet’s population have “äppärät” smartphones.[16] Between 2023 and 2024, the amount of data travelling between these devices and other pieces of ICT infrastructure grew by 25 per cent.[17]

On the downside, these devices may be tracked, monitored, and targeted by technologies that scan the electromagnetic spectrum, inspect data flows on backbone networks, and hacking tools compromising apps and operating system software. On the battlefields of the Russo-Ukrainian War, they have shown to be a huge liability. Presence on cell phone networks along the front lines of that conflict and others is a common trigger for attack and has been for over a decade.[18] That Russian small unit commanders tack mobile phones to the walls of bunkers if they are found among front-line troops, as they did in one viral instance, is solid proof of the vulnerability the technology opens to military units.

One of the more surprising developments of the Russo-Ukraine War is the utility of commercial Internet and cellular technology on the battlefield. That artillery fires are called in via Starlink satellite modem, is but one of the unforeseen developments of that conflict. Keeping tabs on the activities identified as hybrid or “grey zone” conflicts incorporates information from many, many platforms and systems.[19] Included in an ontology of hybrid conflict are: propaganda

A Russian soldier nails confiscated cellphones to a post in 2024.
Source: @clashreport, x.com.

operations, principally undertaken online; official declarations and press reports; computer network attack and defence activity; information regarding military movements and exercises; and economic data (i.e. buying up fuels to prepare for war or manipulating markets to create asymmetric advantage). The goal for states facing acute security issues and responsibilities is, as it was in the early days of the Cold War, to avoid surprise.[20] Avoiding it today means that capacity must grow in analysing the flood of data we call intelligence.

Measuring Hybrid Influence and Action

At a time when the level of hyperbole regarding artificial intelligence (AI) could hardly rise any higher, the human capacity to understand information remains constrained by attention and time. The amount of information on the World Wide Web (www) alone would require more than 200,000 years for a single person to read. The good news for prospective hybrid warfare analysts is that not everything needs to be read, and what does can be accomplished by organisations of professionals. Analytic teams can monitor variables relevant to information operations, but the question is how.[21]

The answer is tripartite, involving (a) identifying key variables; (b) baselining of what we may call “normal” activity; and (c) the weights of different variables in a machine learning algorithm for processing collected data. From this, a framework may emerge for observing change in the exertion of information power.

Understanding hybrid conflict involves the incorporation of manifold areas of knowledge. Much of this is encompassed in what contemporary Western military theorists call the information environment.[22] Putting bounds on that environment is daunting. It is large, much like the physical environment in which it is constructed. Much of the information now exchanged and absorbed by people is digital. This indicates enormous streams and repositories of data. The challenge lies in locating those sources which may better illuminate the exertion of power in the international system. Scholarship on the information dimension of international relations has been approached by methods of news analysis,[23] public declaration,[24] leadership analysis and related political psychology,[25] and now, for some time, Internet communications and interactions.[26] Thanks to the continued durability of Moore’s Law in the growth of computing power, the mechanisms for inquiry in these areas may be re-engineered in light of technological advances.[27]

In the information environment of hybrid warfare, a bridge must be constructed between technical capacity and social response. Advertising may offer a shortcut to valuing information power in international competition and conflict.[28] Technology has revolutionised the ad industry. With the arrival of ubiquitous computing, advertisements delivered by Internet companies such as Alphabet (Google) and Meta (Facebook) target individuals rather than audiences.[29] Spending on political advertising in the U.S. is projected to reach almost $3.5 billion in the 2024 election cycle, while traditional ad spending (TV, radio, print, etc.) is still far more, at some $7.9 billion. The total amount, some $12 billion, represents an increase of nearly a third from the 2020 election cycle. Most of that growth is in what the advertising industry calls “digital.”[30] What the ad industry has labelled digital is a pathway to discovering information power variables.

The largest growth area for political ad spending is in what the advertising industry calls connected television. Connected TV is video delivered by the Internet.[31] Services from Alphabet, Amazon, Netflix, and traditional media companies like Disney deliver these ads to viewers. They appear in an ever-growing flood of video, as some 20 days’ worth of video are uploaded to Alphabet’s YouTube service every minute. In this exponentially growing video archive, propagandists deliver their messages to the public abroad.[32] Interestingly, the Russian government recently blocked its citizens from accessing the service.[33] It appears likely that both video content and the ads surrounding it are a potential threat to some states. These categories of digital data should be tracked by those who observe hybrid conflict as well.

On X (formerly Twitter), Telegram, and Alphabet’s Instagram, many variables, including the metadata produced by those platforms, must be followed by practitioners of active measures.[34] Government officials and political candidates make use of these Internet platforms to communicate their messages.[35] Propagandists are somewhat less up-front about how they spread their narrative views but work with the same technologies.[36] Where once practitioners of active measures covertly published magazines and newsletters, now they create online news and opinions,[37] often with assistance from Large Language Model (LLM) AI models.[38] Situational awareness for hybrid conflict translates to effective monitoring of sources of information designed to influence beliefs. Such activity will likely need to be undertaken for the foreseeable future. Information power still appears to be relevant.

How Does Influence Work in the Hybrid Contest?

To understand whether influence operations work, consider the example of Russia's attempts to isolate Ukraine and deprive it of Western support. Until the U.S. Congress voted to approve a major round of assistance to Ukraine in April 2020, Russian propaganda held up U.S. legislative action on the provision of military aid to Ukraine for months. A recent Breitbart headline, "Exclusive: [House Speaker] Johnson's top policy advisor is former lobbyist…Clients have corporate interest in Ukraine War" is an example of information operations in which pro-Russia actions are camouflaged in the anti-corporate narrative. [39] Sacked Fox News commentator Tucker Carlson interviewed Vladimir Putin in Russia and stuck around to film segments in which he called Moscow, "much nicer than any city in my country."[40] One long-serving Republican member of the U.S. Congress chastised his own caucus for introducing Russian propaganda talking points as fact into the chamber's deliberations.[41]

Hybrid conflict-oriented propaganda targets national politics but also the militaries of targeted countries as well.[42] What this means in practice is their ideological compatibility with missions that may be subject to tremendous political propaganda. False reports of violence by German soldiers serving in Lithuania may be but the tip of the iceberg in anti-NATO digital propaganda undertaken by Russia.[43] Perhaps the best indicator of their effectiveness is the presence of neo-fascistic elements in NATO militaries, and their willingness to work against their own services due to foreign, malign information influence propagated across cyberspace.

While not a military conflict, the COVID-19 pandemic likewise opened the doors for propagandists, including those in the U.S., to manipulate publics online.[44] False narratives fooled the naïve and intellectually impressionable. In some cases, the cost was their lives. Hybrid conflict indicators abound in the information environment, but their presence does not necessarily provide a forecast of future military conflict or covert action. Connecting the dots on information operations in a conflict that may pass from the "grey zone" to significant hostilities is requisite for early warning and efforts at peace. That also means that just because rhetoric between two states may be bellicose doesn't necessarily add up to open conflict. Now toned down, the war of words between Japan and South Korea spoke to an old animosity but not a renewed conflict.

AI's Role in Grasping Understanding in a Sea of Data

ICTs have transformed society, particularly through the rapid proliferation of information. Perhaps the most important observation in the preparation of this essay was an oft-repeated belief that AI answers all questions, removing the need for critical thinking.[45] This could have devastating effects as we learn more about how AI performance can be biased and how that bias may be influenced.[46]

At hand is a tremendous computational capacity for the sensemaking of digital information. The technologies to process information can be incredibly useful in bringing order to the chaos of the information environment.[47] For instance, BERT, a computational-linguistic tool, can be trained to detect online propaganda through its ever-evolving linguistic model.[48] However, for every advance in detecting information operations, the propagandists will also innovate. This is the nature of technologically infused statecraft. When divided into sides, players in the international system attempt to leverage innovation for comparative advantage.

The information components of hybrid conflict can be found and finding them can be partially undertaken by computers. That said, AI is not a panacea. There is perhaps too much talk about AI by those who may not understand how the technology works today or will evolve. However, the evolution of the neural network-machine learning process we call AI is advancing consistently. The head of Google's Deep Mind division, the centre for the company's AI research and development, asserts recently that those advances will continue. He observes: "In recent years, I think machine learning has really changed our expectations of what we think of computers being able to do. If you think back 10 or 15 years ago, speech recognition kind of worked, but it wasn't really seamless – it made lots of errors. Computers didn't really understand images from the pixel level of what was in that image. There was a bunch of work in natural language processing, but it wasn't really a deep understanding of language concepts and multilingual data. But I think we've moved from that stage to one where you actually expect computers to be able to see and perceive the world around us in a much better way than they were able to 10 years ago."[49]

While Dean sees tremendous advances in computer reasoning, the data for understanding information influence or other hybrid warfare tactics will require sophisticated models. One approach is to simulate society at scale. One research group envisages the employment of High Definition Cognitive Models representing the mindset of specific individuals.[50] The challenge with such an approach is to capture the heterodox nature of a population and understand how AI approximation may yield useful observations. Computing advances will continue, but the greater challenge may be structuring and weighting data to construct useful analytic tools. That process, let alone hybrid warfare, is still relatively immature as applied to international relations.

Grow Civilian and Diplomatic Institutions

Hybrid conflict embraces a repertoire of actions that can produce a maximum effect while simultaneously managing escalatory dynamics. The governments of the West's democracies employ diplomatic, intelligence, and military capabilities to maintain peace and offer early warning in a way not seen before the paired catastrophes of two world wars. In the decades since 1945, those organisations have adapted to manifold threats, from denial and disinformation operations to thermonuclear warfare. Assuring security has required the contributions of many actors availing themselves of new technology and tradecraft for necessary adaptation to the methods of intelligent and motivated adversaries.

That adaptation also extends to alterations in the proverbial "rules of the game" in international relations. Deepfakes, kinetic cyberattacks, and transnational criminal-terror syndicates are all realities of the contemporary security environment that would have been labelled science fiction a few decades ago. In addition to new actors and actions, the conflict now plays out on a deeply globalised geographic information tableau upon which advantage is sought while maintaining escalation in check still, a significant challenge remains in directing the attentions attention of computer algorithms to both find and analyse them. Hostile and aggressive states use the tools they have at hand. North Korea, for instance, has learned how to employ cyber tools to perpetrate the first heist of a national reserve bank.[51] The capacity for innovation in a digitally interconnected world is a source of regular surprise for the community of states seeking a norms-based international order that promotes shared interests and collective security. Staying apprised of that innovation, undertaken by a growing club of authoritarian regimes increasingly willing to collaborate, is an utmost priority.

If there is a defining attribute of our time, it is how societies can cope with torrents of information to make sense of the world they inhabit. The information environment grows exponentially. Tracking what goes on within it will be the job of

practitioners in many disciplines who are able to cooperate in making sense of the perception we call security. Journalists, academics and concerned citizens will be at the vanguard of discovery for hybrid warfare information operations. In the Global West, governments shouldn't get a pass just because these actors are present and capable, however. While military alliances are built on the cooperation of armed forces, Western democracies would be wise to grow civilian and diplomatic institutions for hybrid conflict in the digital domain.

What this will mean is probably a further erosion of institutional or organisational silos related to security. Police, spies, soldiers, corporations and interested citizens of all stripes will contribute to sensemaking in a world marked by hybrid conflicts. How that collaboration will function is very much a work in the earliest phases of progress. Perhaps the most important question for identifying the machinations of hybrid warfare is what it will cost, in both blood and treasure, those who wish to deter it.

Endnotes

[1] Edward Hallett Carr, The twenty years' crisis, 1919-1939: Reissued with a new preface from Michael Cox, Springer, 2016.

[2] Joseph S. Nye, The future of power, Public Affairs, 2011.

[3] Herbert A. Simon, "Notes on the observation and measurement of political power," The Journal of Politics 15, no. 4 (1953): 500-516.

[4] Sub-areas of hybrid conflict can include cyber activity, terrorism, information operations, international crime, and economic activity. Frank G. Hoffman, "Hybrid warfare and challenges," In Strategic Studies, 329-337. Routledge, 2014.

[5] Margret S. MacDonald and Anthony G. Oettinger, "Information overload," Harvard International Review 24, no. 3 (2002): 44.

[6] Erhard Rahm and Hong Hai Do, "Data cleaning: Problems and current approaches," IEEE Data Eng. Bull. 23, no. 4 (2000): 3-13.

[7] Zheng Xu, Lin Mei, Kim-Kwang Raymond Choo, Zhihan Lv, Chuanping Hu, Xiangfeng Luo, and Yunhuai Liu, "Mobile crowd sensing of human-like intelligence using social sensors: A survey," Neurocomputing 279 (2018): 3-10.

[8] Aaron F. Brantly, "Ukraine War OSINT Analysis: A Collaborative Student Report," (2023).

[9] Generating intelligence from social media was defined almost a decade ago. OSINT has been discussed significantly since the 1990s. Laura K. Donohue, "The dawn of social intelligence (SOCINT)," Drake L. Rev. 63 (2015): 1061.

[10] Chris Bronk, Gabriel Collins, and Dan S. Wallach, "The Ukrainian Information and Cyber War," The Cyber Defense Review 8, no. 3 (2023): 33-50.

[11] Brent D. Sadler, "Applying Lessons of the Naval War in Ukraine for a Potential War with China," Backgrounder 3743 (2023): 1-13.

[12] Alex Roland and Philip Shiman, Strategic Computing: DARPA and the quest for machine intelligence, 1983-1993, MIT Press, 2002.

[13] Ronald J. Deibert, Reset: Reclaiming the Internet for civil society. House of Anansi, 2020.

[14] Muhammad Sarwar and Tariq Rahim Soomro, "Impact of smartphones on society," European Journal of Scientific Research 98, no. 2 (2013): 216-226.

[15] https://www.weforum.org/agenda/2023/04/charted-there-are-more-phones-than-people-in-the-world/.

[16] The term "äppärät" is borrowed from Gary Shteyngart's Super Sad True Love Story, a 2011 novel set in a dystopian near future where mobile devices were all-consuming of human attention. Sounds crazy. Gary Shteyngart, Super sad true love story: A novel. Random House Trade Paperbacks, 2011.

[17] This data traffic growth of 25 per cent a year is a staggering statistic and has held true for more than a decade. Fredrik Jejdling, Ericsson Mobility Report 2024. June 2024.

[18] Chris Bronk and Gregory S. Anderson, "Encounter battle: Engaging ISIL in cyberspace," The Cyber Defense Review 2, no. 1 (2017): 93-108.

[19] Michael J. Mazarr, "Mastering the gray zone: understanding a changing era of conflict," US Army War College (2015).

[20] Roberta Wohlstetter, Pearl Harbor: warning and decision. Stanford University Press, 1962.

[21] The value of AI technologies to analytic teamwork is in its earliest phases. Lauro Snidaro, "ChatGPT Act as an Intelligence Officer," In 2023 IEEE International Workshop on Technologies for Defense and Security (TechDefense), 449-454. IEEE, 2023.

[22] Michelangelo Conoscenti, "The Military's Approach to the Information Environment," In The Routledge Handbook of Discourse and Disinformation, 218-238. Routledge, 2023.

[23] Kalev Leetaru and Philip A. Schrodt, "Gdelt: Global data on events, location, and tone, 1979-2012," In ISA annual convention, vol. 2, no. 4, 1-49. Citeseer, 2013.

[24] Gavan Duffy and Brian Frederking, "Changing the rules: A speech act analysis of the end of the Cold War," International Studies Quarterly 53, no. 2 (2009): 325-347.

[25] Margaret G. Hermann and Charles W. Kegley Jr., "Rethinking democracy and international peace: Perspectives from political psychology," International Studies Quarterly 39, no. 4 (1995): 511-533.

[26] Charli Carpenter and Daniel W. Drezner, "International Relations 2.0: The implications of new media for an old profession," International Studies Perspectives 11, no. 3 (2010): 255-272.

[27] Mark S. Lundstrom and Muhammad A. Alam, "Moore's law: the journey ahead," Science 378, no. 6621 (2022): 722-723.

[28] Garrett A. Johnson, Randall A. Lewis, and David H. Reiley, "When less is more: Data and power in advertising experiments," Marketing Science 36, no. 1 (2017): 43-53.

[29] Ritam Dutt, Ashok Deb, and Emilio Ferrara, ""Senator, We Sell Ads": Analysis of the 2016 Russian Facebook Ads Campaign," In Advances in Data Science: Third International Conference on Intelligent Information Technologies, ICIIT 2018, Chennai, India, December 11-14, 2018, Proceedings 3, 151-168. Springer Singapore, 2019.

[30] Trade press publications can offer some interesting insights. The $12 billion ad spend is an amount roughly the size of Guyana's GDP. "2024 Political Ad Spending Will Jump Nearly 30% vs. 2020," EMarketer, January 11, 2024, https://www.emarketer.com/press-releases/2024-political-ad-spending-will-jump-nearly-30-vs-2020/.

[31] Paul Murschetz, "Connected television: Media convergence, industry structure, and corporate strategies," Annals of the International Communication Association 40, no. 1 (2016): 69-93.

[32] Robert W.Orttung and Elizabeth Nelson, "Russia Today's Strategy and Effectiveness on YouTube," Post-Soviet Affairs 35, no. 2 (2019): 77-92.

[33] Alexander Marrow and Gleb Stolyarov, "YouTube slowdown in Russia darkens freedom of speech outlook," Reuters. August 08, 2024. YouTube was blocked by China years ago.

[34] Mylynn Felt, "Social media and the social sciences: How researchers employ Big Data analytics," Big data & society 3, no. 1 (2016): 2053951716645828.

[35] Jason Gainous and Kevin M. Wagner, Tweeting to power: The social media revolution in American politics, Oxford University Press, 2014.

[36] Yevgeniy Golovchenko, Cody Buntain, Gregory Eady, Megan A. Brown, and Joshua A. Tucker, "Cross-platform state propaganda: Russian trolls on twitter and YouTube during the 2016 US Presidential Election," The International Journal of Press/Politics 25, no. 3 (2020): 357-389.

[37] Thomas Rid, Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux, 2020.

[38] Paweł Golik, Arkadiusz Modzelewski, and Aleksander Jochym, "DSHacker at CheckThat! 2024: LLMs and BERT for Check-Worthy Claims Detection with Propaganda Co-occurrence Analysis," (2024).

[39] Wendell Husebø and Matthew Boyle, "Exclusive-Mike Johnson's top policy adviser is former lobbyist: clients have interest in Ukraine War," Breitbart, April 17, 2024.

[40] Dominick Mastrangelo, "Tucker Carlson: Moscow 'so much nicer than any city in my country'," The Hill, February 13, 2024.

[41] Julia Ioffe, "McCaul to Action," Puck, April 02, 2024, https://puck.news/ukraine-aid-q-and-a-rep-mccaul-on-republican-support-for-bill/.

[42] Christopher Paul and Miriam Matthews, "The Russian "firehose of falsehood" propaganda model," Rand Corporation 2, no. 7 (2016): 1-10.

[43] "Fake news campaign targets German Army," DW. February 16, 2017.

[44] Chris Bing and Joel Schectman, "Special Report: How U.S. Taxpayers Funded a 'Global Propaganda' Program to Push Covid-19 Vaccine Abroad," Reuters, July 25, 2023.

[45] Claire Su-Yeon Park, Haejoong Kım, and Sangmin Lee, "Do less teaching, do more coaching: toward critical thinking for ethical applications of artificial intelligence," Journal of Learning and Teaching in Digital Age 6, no. 2 (2021): 97-100.

[46] Reva Schwartz, Apostol Vassilev, Kristen Greene, Lori Perine, Andrew Burt, and Patrick Hall, Towards a standard for identifying and managing bias in artificial intelligence. Vol. 3., U.S. Department of Commerce, National Institute of Standards and Technology, 2022.

[47] Stephen L. Dorton and Robert A. Hall, "Collaborative human-AI sensemaking for intelligence analysis," In: International conference on human-computer interaction, 185-201, Cham: Springer International Publishing, 2021.

[48] For more information on BERT: Mikhail V. Koroteev, "BERT: a review of applications in natural language processing and understanding," arXiv preprint arXiv:2103.11943 (2021).

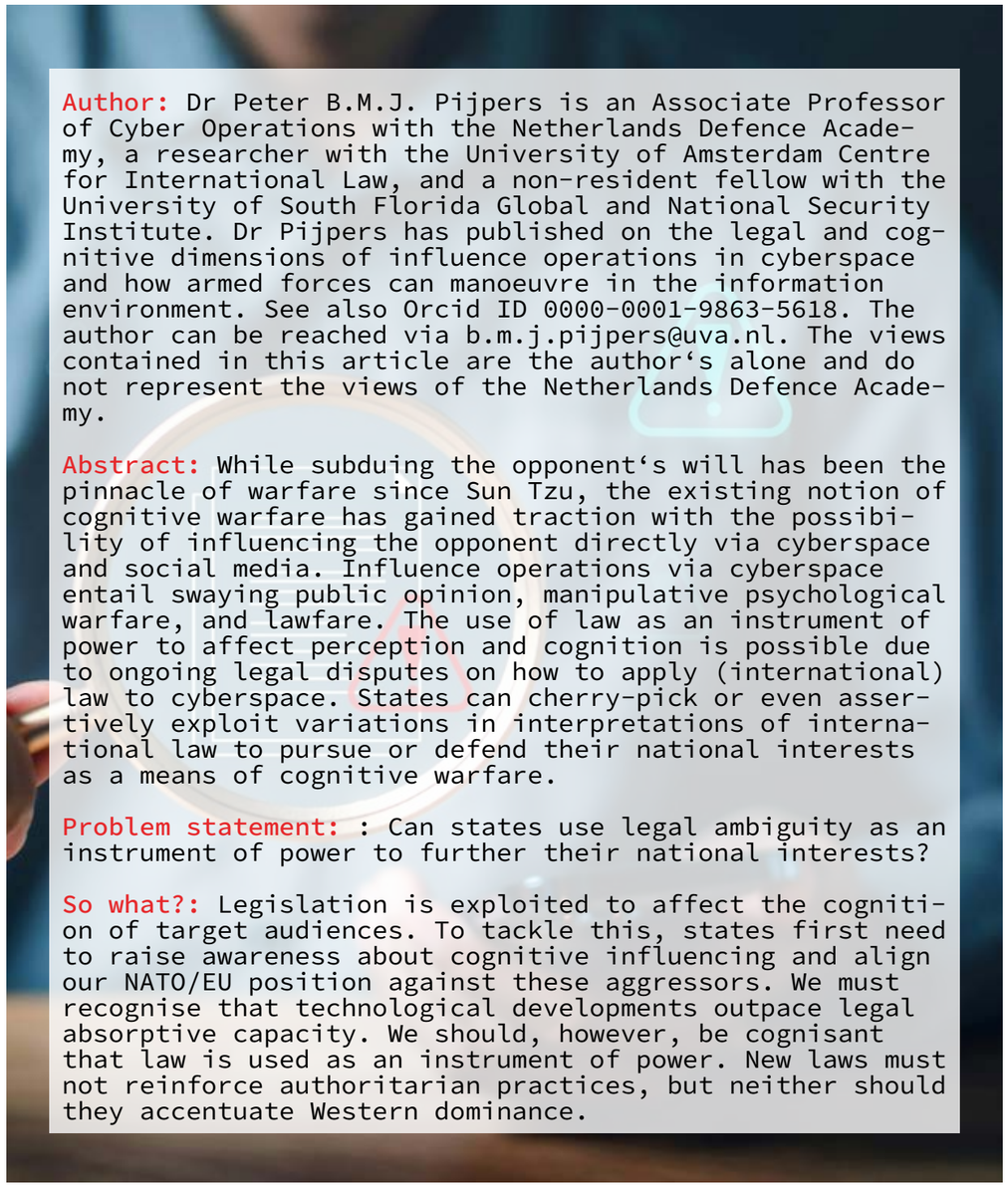
[49] Jeff Dean, "Exciting Trends in Machine Learning," (Lecture), Rice University, Houston, TX, February 13, 2024.

[50] Michael Bernard, George Backus, Matthew Glickman, Charles Gieseler, and Russel Waymire, "Modeling Populations of Interest in Order to Simulate Cultural Response to Influence Activities," In Social Computing and Behavioral Modeling, 1-8. Springer U.S., 2009.

[51] Seongjun Park, "Evading, Hacking & Laundering for Nukes: North Korea's Financial Cybercrimes & the Missing Silver Bullet for Countering Them," Fordham Int'l LJ 45 (2021): 675.

Legislation As An Instrument Of Cognitive Warfare

PETER B.M.J. PIJPERS



Author: Dr Peter B.M.J. Pijpers is an Associate Professor of Cyber Operations with the Netherlands Defence Academy, a researcher with the University of Amsterdam Centre for International Law, and a non-resident fellow with the University of South Florida Global and National Security Institute. Dr Pijpers has published on the legal and cognitive dimensions of influence operations in cyberspace and how armed forces can manoeuvre in the information environment. See also Orcid ID 0000-0001-9863-5618. The author can be reached via b.m.j.pijpers@uva.nl. The views contained in this article are the author‘s alone and do not represent the views of the Netherlands Defence Academy.

Abstract: While subduing the opponent‘s will has been the pinnacle of warfare since Sun Tzu, the existing notion of cognitive warfare has gained traction with the possibility of influencing the opponent directly via cyberspace and social media. Influence operations via cyberspace entail swaying public opinion, manipulative psychological warfare, and lawfare. The use of law as an instrument of power to affect perception and cognition is possible due to ongoing legal disputes on how to apply (international) law to cyberspace. States can cherry-pick or even assertively exploit variations in interpretations of international law to pursue or defend their national interests as a means of cognitive warfare.

Problem statement: : Can states use legal ambiguity as an instrument of power to further their national interests?

So what?: Legislation is exploited to affect the cognition of target audiences. To tackle this, states first need to raise awareness about cognitive influencing and align our NATO/EU position against these aggressors. We must recognise that technological developments outpace legal absorptive capacity. We should, however, be cognisant that law is used as an instrument of power. New laws must not reinforce authoritarian practices, but neither should they accentuate Western dominance.

Influence the Will: An Introduction

In May 2024, Annalena Baerbock, German Federal Minister for Foreign Affairs, attributed a cyberattack on the German Social Democratic Party (SPD) to APT 28, an agent of the Russian Military Intelligence Service, the GRU.[1] The attack, most likely a spear-phishing attack, was part of a broader campaign to undermine the June 2024 European (EU) elections. Similarly, NATO's North Atlantic Council expressed concerns as it witnessed subversive and undermining cyberattacks against the Baltic states, Poland, and the United Kingdom.

Elections are precarious periods for democracies; they are conceptual seams where a society moves from one set of elected lawmakers to another. In any system, whether organising a military campaign or welding a heating system, seams pose vulnerabilities. Liberal democracies have more vulnerabilities—since there are more seams in a democratic system—than authoritarian states, where there is often no genuine division of power, let alone a change of power.

Influencing the people's will through elections has long been part of the game plan in the bipolar Cold War. The Soviet Active Measures and American Political Warfare covered election interference to persuade or manipulate the cognition of foreign audiences and political leaders to elect or put in place a government in line with Soviet or U.S. interests, respectively.

While subduing the opponent's will has been the pinnacle of warfare since Sun Tzu, the notion of cognitive warfare has gained traction with the growth of cyberspace and the possibility of influencing opposing audiences directly via social media. Cyberspace is a man-made domain that has added three layers to the existing information environment: the hardware itself, the virtual persona we use to communicate online, and the data and protocols that make communication possible.[2] These additional layers provide new target surfaces that state and non-state actors will want to protect or use, to engage with others.

The dawn of cyberspace has enabled three cyber-related categories of activities: Digital intelligence gathering (espionage) through scanning or copying of data confined in virtual repositories, subversive digital influence operations,[3] and digital undermining.[4] The latter cyber-attacks are activities in the virtual dimension that undermine cyberspace with binary code, modify or manipulate data, and degrade or destroy the hardware or protocols, resulting in virtual and/or physical effects in cyberspace. Digital influence operations use cyberspace as a vector (without affecting it) to target the (human) cognitive dimension of groups or audiences, making use of content, words, memes, and footage as 'weapons'.[5] Apart from large state-supported activities such as Stuxnet in the past, most cyberattacks witnessed in Ukraine and Gaza have had limited impact. Conversely, state-level influence operations, including the Russian interference during the 2016 U.S. presidential election, did had strategic effects.[6]

Apart from the activities in cyberspace, the wars in Ukraine and Gaza witnessed new actors and technologies emerging. Non-state actors, including Anonymous, Microsoft, and Elon Musk, play a role in these conflicts without becoming a belligerent party, and artificial intelligence is used in targeting systems in the Gaza war.[7] These topics raise not only operational and ethical questions but also legal ones, for example, on DDoS attacks by a non-state actor and the international humanitarian law (IHL) or the IHL article 49 AP1's coverage of cyber attacks.[8]

Using or exploiting varying interpretations states have on (international) law can even be used as an instrument of power to affect perception and cognition. This form of 'lawfare'[9] can be a tool in influencing the cognition of target audiences through

cyberspace. States can cherry-pick or assertively exploit the variations in interpretations of international law to pursue or defend their national interests as a means of cognitive warfare.

What is Cognitive Warfare?

From a security or military perspective, the cognitive domain is the pinnacle of warfare. Thinkers such as Thucydides or Von Clausewitz argue that the essence of warfare is to subdue an enemy—meaning making sure that the opposite actor (willingly or unwillingly) becomes convinced that it should change its behaviour and act under our will.

In the past, the cognitive domain was influenced by physical acts, hence indirectly via the (threat of the) destruction of armies or capitals. With the inception of cyberspace and the increased knowledge of cognitive psychology,[10] cognitive warfare nowadays also directly targets the mind, making use of influence operations, information operations, and psychological warfare—hence, warfare without the use of kinetic force. Cognitive activities can be applied to persuade our conscious mind. However, their focus is on exploiting our subconscious mind,[11] the main drivers of our behaviour: biases, heuristics, intuition, and emotions.

As a conceptual notion, cognitive warfare cannot be easily defined. In a research paper by Cluzel, cognitive warfare is compared to hacking the minds of individuals to 'erode the trust that underpins every society', which includes the use of neuroscience and technology.[12] Hung and Hung argue that information warfare is a subset of cognitive warfare,[13] and influence operations are merely the cyber-related elements of information warfare. Others argue the opposite, stating that 'cognitive warfare has absorbed information warfare'.[14] In both cases, there is a shift from controlling the media (information) to controlling the brain (cognition). NATO's proposed definition is 'Deliberate, synchronised military and non-military activities throughout the continuum of competition designed to affect audience attitudes, perceptions and behaviours to gain, maintain and protect cognitive superiority.'[15] Other definitions of cognitive warfare argue that cognitive warfare is a strategy that focuses on altering how a target population thinks and how it acts through that. Or they claim that 'in cognitive warfare, the ultimate aim is to alter our perception of reality and deceive the brain in order to affect our decision-making.'[16] In all definitions and descriptions of cognitive war, trust and truth are the primary targets.[17]

Cognitive Warfare via Cyberspace

With the growth of cyberspace, our societies havebecome more digitalised, but also warfare is digitalised. The potential and actual impact of cyber activities is widely debated. Though some scholars argue that cyberwarfare equals regular warfare, a more common view is that most cyber-operations will not reach the threshold of war. This means that labelling cyber-operations will benefit from looking at the effects they might have rather than the act itself.[18]

A recent example of large-scale cyber activities is the Russia-Ukraine war. Since the start of the invasion in February 2022, more than 3,500 attacks have taken place.[19] Various actors, including states, have undertaken these attacks. However, 95% of the attacks can be labelled as DDoS, defacements, or hack (& leak) operations. And some 90% of these were executed by non-state actors. DDoS and defacements are what Gartzke & Lindsay would categorise as hindrances or nuisances,[20] causing neither 'death and destruction' nor directly supporting a military campaign. Though some cyber-attacks supported operational-level military or diplomatic campaigns, including digital espionage or severe wiperware attacks, no cyber-attacks with severe strategic impact (similar to a cyber Pearl Harbour) have been registered.

Despite the scale, the impact of cyberspace activities in the Russia-Ukraine war appears to be marginal, possibly due to Ukrainian resistance, resilience (supported by firms such as Microsoft), and faltering Russian operations. There are, however, some notable exceptions, as some cyber operations did serve their purpose. First, on the eve of the invasion, Russia attacked the 'Viasat' satellite internet connection, imposing a digital blackout on Ukrainian forces. Second is the fervent online strategic communication by Ukrainian President Zelensky to foreign parliaments that has resulted in diplomatic support and the supply of funds, military systems, and ammunition.

Contrary to undermining cyber-attacks, digital influence operations can have strategic effects. While influence operations are not inherently malign, they intend to affect deliberate understanding and autonomous decision-making processes of humans or groups in a conscious or preferably subconscious manner. In the end, cognitive warfare via influence operations in cyberspace does not aim at the destruction of humans but at 'reformatting' the target audience with values, morality and the understanding of good and evil in line with what the attackers want.[21]

Since the annexation of Crimea, pro-Russian state and non-state actors conducted cyber-enabled disruptive propaganda and disinformation campaigns to create an information environment in which confronting views and perceptions exist.[22] The main purpose of Russian 'information confrontation'[23] operations is to demoralise the Ukrainian population and to drive a wedge between Ukraine and its Western allies. Influence operations are also used to target domestic Russian audiences. Narratives used are Western Russo-phobia, the 'denazification and demilitarisation' of Ukraine or the endemic corruption within the Ukrainian government.[24] Ukraine similarly exploits social media. From the invasion on, President Zelensky has addressed his population online and kept up the morale of his troops, positively affecting the cognitive dimension of both friend and foe.[25] For Ukraine, international support is its lifeline and thus a centre of gravity, but consequently also an Achilles' heel.[26]

Influence operations, especially manipulative ones, are inherently deceptive and use heuristics and biases, luring the target audience away from a rational decision-making process in favour of what Petty and Cacioppo call the peripheral route.[27] The peripheral route is invoked by luring a targeted audience towards a socially divisive topic, impairing their ability to process incoming data due to the emotional or provocative sentiment attached. Hung and Hung make a similar assessment, arguing that cognitive warfare uses two dimensions: the psychological techniques (how our brain works) based on heuristics and repeated stimulation and, second, the cognitive handling of external information. To influence humans, a gap (or 'free energy') needs to exist—or to be created—between prior predictions and incoming stimuli; in effect, the target audience needs to start doubting, which is in line with the Russian approach of information confrontation.[28]

Western democracies are more vulnerable to manipulative influence operations as an element of cognitive warfare - and hence for Russian information confrontation - due to their open societies, built on the freedom of speech, of press, and freedom to vote and be elected. Notions that are embedded in the principles of legality and legitimacy go hand in hand with the trust people have in the government, judges, and traditional (often written) media. Western democracies entirely use free energy to discuss and absorb incoming stimuli, create new ideas, innovate, fail, and learn. This is in contrast to authoritarian states that try to undermine incoming (foreign) stimuli, information and new ideas and make sure that the inoculated perception (or prior beliefs) of the population is aligned with the (state-controlled) information environment and not distorted by (false or factual) evidence that will change the prior belief and create doubt.

Legislation in Cognitive Warfare

In addition to the example of Russia's information confrontation, the Chinese Three Warfares is another example of cognitive warfare. This doctrine, governed mainly by the Chinese Communist Party's (CCP) United Front Work Department[29] and the People's Liberation Army,[30] aims to maintain the CCP's political power and 'control the prevailing discourse and influence perceptions to advance China's interest'.[31] To suppress incoming stimuli and propagate a benign image of the People's Republic of China (PRC), diasporas are dissuaded to voice dissenting opinions. The Internet and social media are frequently censored domestically.[32] The Three Warfares doctrine not only entails a persuasive and manipulative but also a legal perception on how to change the attitude and, hence, the behaviour of targeted audiences—at home or abroad.[33]

Persuasive public opinion warfare, or media warfare, aims to shape 'targeted audiences through information derived and propagated by mass information channels,' traditional (television, newspaper, movies) and the Internet.[34] Public opinion warfare relates to shaping (online) public opinion to transmit a consistent message to the targeted audience in a way favourable to Chinese positions.[35]

Where public opinion warfare focuses on framing or highlighting some aspects of the truth and neglecting others, often with a pinch of humour, psychological warfare is more manipulative in nature. Psychological warfare involves using information to pressure an opponent and 'create damaging or deleterious habits and ways of thinking, to reduce its will to resist, and perhaps even to induce defeatism and surrender.'[36] Psychological warfare makes use of a variety of techniques, including intimidation, religious interference,[37] dissuasion, manipulation, and deception.[38]

Interestingly, the Chinese Three Warfares are applicable in all phases of conflict (from peace to war) and make use of diverging legal interpretations to influence others. Legal warfare is designed 'to justify a course of action,[39] forging a normative environment favourable to China. The PRC's legal warfare, which echoes Western debates on lawfare,[40] is a tool of non-kinetic warfare that offers influence over an actor's behaviour to achieve strategic ends. Successful legal warfare limits others' freedom of movement while expanding the PRC's freedom of action.[41]

Three Warfares is not a specific policy of the CCP. The effectiveness of the Three Warfares lies in the fact that it is a society-wide endeavour. When addressing foreign audiences, the Three Warfares activities make use of the PRC's entire media landscape so that a given message is reiterated and reinforced by different sources and different versions. Outlets include media channels (CGTN), cultural institutes (Confucius Institutes), Chinese exchange students,[42] diaspora communities, think tanks and the Chinese diplomatic network to affect foreign audiences.[43]

Law as an Instrument of Warfare

The PRC's legal warfare exploits the ambiguity in international law related to new developments, a discourse that is not new. Nuclear weapons or aeroplanes were introduced after the Laws of Armed Conflict (IHL) were conceived. However, since (international) law is based on principles including military advantage, distinction, proportionality, and necessity, not on specific situations or techniques, the law will still apply. In practice, a discourse will start on how to apply the existing international law to the new development, for instance, in the United Nations Group of Governmental Experts or the Open-Ended Working Group.[44]

On the one hand, since international law is based on principles from which rules derive, it has always been the purpose of the body of international law to provide legal room to manoeuvre so generic rules can be applied to a specific situation or new developments.[45] On the other hand, new developments can cause challenges, not least due to the speed of (technological) developments, including artificial intelligence,[46] human enhancement, drones or cyberspace. This parallax causes uncertainty regarding how to apply the law. In cyberspace, there is debate on whether sovereignty—a legal obligation in traditional international law—is a rule (obligation) and principle or merely a principle of law; the latter is the UK position. This is not a semantic discussion because if sovereignty is a principle—hence not an obligation—it cannot be violated. The articles on State Responsibility state that an Internationally Wrongful act constitutes a breach of a primary rule of law (an obligation) that can be attributed to a state. If sovereignty is breached by a state that does not see it as an obligation, the redress or countermeasure could be a violation of international law, in which case a row could escalate into a conflict.

Another source of ambiguity is whether cyberspace, as such, is part of the territory of a state or not, and thus subject to its laws. In many Western views, territory includes the soil, the territorial sea and the air column above it. Hence, not space in general or the virtual aspects of cyberspace—the zeros and ones.[47] In that sense, the virtual dimension of cyberspace is borderless. In many authoritarian states cyberspace in total is linked to the control of territorial integrity. Hence, the PRC will argue that it has digital sovereignty over cyberspace 'on its soil' while Western states only have territorial control over the hardware on its soil.

Moreover, while Western states argue that international law supersedes national law, the Russian constitution argues that national law has prerogative over international law. Conversely, the PRC uses internatio-

nal law to underline their claims, e.g., in the South China Sea,[48] and will dispute the Western view that solely natural (and not artificial) islands are part of a territorial claim.

Finally, for the CCP, a clear distinction between war and peace does not exist. Based on the Three Warfares, these forms of 'warfare' commence before actual military engagement and are conducted to shape and prepare the battlefield and its participants. All these forms of the Three Warfares are applicable across the entire spectrum of war and peace.

How to Counter The Use of Lawfare

The use of law as an instrument of power to affect perception and cognition is possible since there are ongoing legal disputes, and states hold varying interpretations on how to apply (international) law to cyberspace. To effectively counter activities of cognitive warfare, it is critical to understand the aggressor's intent before responding. NATO and EU states must raise public awareness of possible foreign cognitive warfare activities, including lawfare, align common positions within the alliances, and finally, a discourse on whether new law is needed remains valid.

First, states, especially liberal democracies, need to realise that Chinese and Russian cognitive warfare differ in intent and depth. Russian activities are meant to sow confusion via the dissemination of information that conflicts or confronts existing knowledge. An example of this was the firehose of falsehoods that followed Russia's downing of MH-17. Russian cognitive and influence operations can be seen as a blunt instrument affecting audiences in foreign states with no other intent than to confuse, sow discord, and undermine trust in democratic foundations. While Russia exploits the variances of international law, it would rather neglect it altogether.

Conversely, Chinese activities are subtle in nature and clearly intend to uphold or improve foreign audiences' benign image of the PRC. The PRC is reliant on international law but favours a renegotiation of its foundations since, according to the PRC, the current body of international law is a reflection of Western interests. In countering the cognitive activities of Russia or the PRC, the intent of the aggressor needs to be considered. The worst mistake to make is to assess the cognitive act according to Western standards.

Raising awareness is (in general) an effective means to counter cognitive warfare. The U.S. citizens were unaware of the impact social media campaigns by foreign actors could have in the run-up to the 2016 presidential election. A naivety that had already largely vanished with the 2018 mid-term elections. Free access to education is pivotal, and where this is already the case, educational programs for schools on the advantages and dangers of an open and free (hence unfiltered) internet.

Besides raising awareness, coalition alignment can also block foreign cognitive warfare, meaning formulating a common position and forming a common bloc among NATO/EU member states with partners, including Japan and Australia. Adversaries will make use of the seams in these coalitions, especially when there is no common rationale, as we currently see in the fragile alignment and hence increased friction within the varying positions of NATO/EU member states regarding the Ukraine war.[49]

Most international legal scholars will argue that current law is sufficient. Still, refinement is needed on how to apply the law for which more state practice and legal statements (opinio iuris) by states are needed. There is a danger that this is wishful thinking. It will be a real challenge to align the diverging opinions of states—as sound legal opinions or as a reflection of political pragmatism. Some states are already entrenched or have seen the benefits of using law as an instrument of power, e.g. during UN/OEWG sessions.

Moreover, new developments (AI, quantum computing) are more complex than they were in the past, and international law can no longer keep the same pace as new developments. EU lawmakers are not yet able to fully grasp the potential and the danger of developments such as AI. However, they correctly see the need for legislation. The result of which are laws that first and foremost reflect the consensus building of the legislative process but will be highly ambiguous in content, which in turn fuels the legal cherry picking and hence the use of law as an instrument of power—a devil's dilemma.

Endnotes

[1] APT means an advanced persistent threat (usually a state (financed) cyber actor), GRU stands for the Russian military intelligence service. See: Marcel Rosenbach & Christophe Schult, “Baerbocks Digitaldetective decken russische Lügenkampagne auf,” Der Spiegel, January 26, 2024, https://archive.ph/2024.01.26-114242/https://www.spiegel.de/politik/deutschland/desinformation-aus-russland-auswaertiges-amt-deckt-pro-russische-kampagne-auf-a-765bb30e-8f76-4606-b7ab-8fb9287a6948.

[2] Peter B.M.J. Pijpers, “Careful What You Wish For: Tackling Legal Uncertainty in Cyberspace,” Nordic Journal of International Law 92, no. 3 (2023), 397-399.

[3] Andreas Krieg, Subversion: The Strategic Weaponization of Narratives, 2023.

[4] Peter B.M.J. Pijpers and Kraesten L. Arnold, “Conquering the Invisible Battleground,” Atlantisch Perspectief 44, no. 4 (2020), 11-14; Paul A.L. Ducheine, Peter B.M.J. Pijpers, and Kraesten L. Arnold, “The ‘Next’ War Should Have Been Fought in Cyberspace, Right?,” in Beyond Ukraine, Debating the Future of War, eds. Tim Sweijs and Jeff Michaels (Hurst Publishers, 2024).; Paul A.L. Ducheine, Jelle van Haaster, and Richard van Harskamp, “Manoeuvring and Generating Effects in the Information Environment,” in Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crisis - NL ARMS 2017, ed. Paul A.L. Ducheine and Frans P.B. Osinga, 2017.

[5] Miranda Lupion, “The Gray War of Our Time: Information Warfare and the Kremlin’s Weaponization of Russian-Language Digital News,” Journal of Slavic Military Studies, 2018, 31 no 3, 329-330; Calder Walton, “What’s Old Is New Again: Cold War Lessons for Countering Disinformation,” Texas National Security Review, Fall 2022.

[6] Ellen Nakashima, “Pentagon Launches First Cyber Operation to Deter Russian Interference in Midterm Elections,” The Washington Post, 2018, https://www.washingtonpost.com/world/national-security/pentagon-launches-first-cyber-operation-to-deter-russian-interference-in-midterm-elections/2018/10/23/12ec6e7e-d6df-11e8-83a2-d1c3da28d6b6_story.html.

[7] Yuval Abraham, “‘Lavender’: The AI Machine Directing Israel’s Bombing Spree in Gaza,” +972 Magazine, no. April (2024), https://www.972mag.com/lavender-ai-israeli-army-gaza/.

[8] Article 49.1. of the 1977 Additional Protocol (1) to the Geneva Conventions states: ‘„Attacks“ means acts of violence against the adversary, whether in offence or in defence’.

[9] Orde F. Kittrie, Lawfare: Law as a Weapon of War (Oxford University Press, 2016), 4-8.

[10] Francois du Cluzel, “Cognitive Warfare” (Innovation Hub, 2021), 12.

[11] Cornelus van der Klaauw, “Cognitive Warfare,” In: The Three Swords no. 39 (2023), 99.

[12] Francois du Cluzel, “Cognitive Warfare,” 7.

[13] Tzu-chieh Hung and Tzu-wei Hung, “How China’s Cognitive Warfare Works : A Frontline Perspective of Taiwan’s Anti-Disinformation Wars,” Journal of Global Security Studies 7, no. 4 (2020), 2-4.

[14] Russtrat, “Cognitive Warfare : War of a New Generation,” Institute of Russian Strategies, December 24, 2021, https://russtrat.ru/en/analytics_/24-december-2021-2228-7813.

[15] NATO Cognitive Warfare Concept, version of April 17, 2024, Supreme Allied Command Transformation.

[16] Cornelus van der Klaauw, “Cognitive Warfare,” 100.

[17] Alonso Bernal et al., “Cognitive Warfare: An Attack on Truth and Thought,” NATO & John Hopkins, 2020; Francois du Cluzel, “Cognitive Warfare,” (Innovation Hub, 2021), 8-9.

[18] Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd ed. (Cambridge University Press, 2017).

[19] CyberPeaceInstitute, “Cyber Dimensions of the Armed Conflict in Ukraine” (2023), https://cyberconflicts.cyberpeaceinstitute.org.

[20] Jon Lindsay and Erik Gartzke, “Coercion through Cyberspace : The Stability-Instability Paradox Revisited,” The Power to Hurt: Coercion in Theory and in Practice, 2016, 179-203.

[21] Russtrat, “Cognitive Warfare : War of a New Generation.”

[22] Todd C. Helmus et al., Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe, Rand Corporation, 2018, 7-25.

[23] Michelle Grisé et al., Russian and Ukrainian Perspectives on the Concept of Information Confrontation, Rand Research Report, 2022, 5-10.

[24] Tine Molendijk “Morale and Moral Injury among Russian and Ukrainian Combatants,” in Reflections on the Russian-Ukrainian War, ed. Maarten Rothman, Lonneke Peperkamp, and Sebastiaan Rietjens (Leiden University Press, 2024), 99-106.

[25] The story of a Ukrainian fighter pilot, ‘the Ghost of Kyiv’, went viral online. Another occurrence concerned the bold response of Ukrainian troops defending Snake Island after Russia’s Black Sea Fleet flagship ‘The Moskva’ demanded their surrender or the attack on the Kerch bridge.

[26] Paul A.L. Ducheine, Peter B.M.J. Pijpers, and Kraesten L. Arnold, “The ‘Next’ War Should Have Been Fought in Cyberspace, Right?,” 101-104.

[27] Richard E. Petty and John T. Cacioppo, “The Elaboration Likelihood Model of Persuasion,” Advances in Experimental Social Psychology 19 (1986), 126.

[28] T.S. Allen and A.J. Moore, “Victory without Casualties: Russia’s Information Operations” Parameters 48, no. 1 (2018), 60.

[29] Marcel Angliviel de la Beaumelle, “The United Front Work Department: ‘Magic Weapon’ at Home and Abroad,” China Brief 17, no. 9 (2017).

[30] But not solely: The ministry of State Security, the Taiwan Affairs office, and the Central Committee of the Party (international liaisons, propaganda and the United Front work department) are involved to name but a few.

[31] Pieter Zhao, “Chinese Political Warfare: A Strategic Tautology? The Three Warfares and the Centrality of Political Warfare within Chinese Strategy,” The Strategy Bridge, no. August (2023), https://thestrategybridge.org/the-bridge/2023/8/28/chinese-political-warfare-a-strategic-tautology.

[32] Alina Polyakova and Chris Meserole, “Exporting Digital Authoritarianism: The Russian and Chinese Models,” Policy Brief, Democracy and Disorder Series, 2019, 1-22, 2-6.

[33] Albert Zhang, “Gaming Public Opinion Influence Operations,” ASPI Policy Brief no. 71 (2023).

[34] Dean Cheng, Cyber Dragon: Inside China’s Information Warfare and Cyber Operations, (Praeger, 2017) 51-53; Peter Mattis, “China’s ‘Three Warfares’ in Perspective,” War On The Rocks, 2023.

[35] See e.g.: CGTN Official, “Samarland, Listed by UNESCO as a World Heritage Site,” X (Twitter), 2023, https://twitter.com/cgtnofficial/status/1707625764412440805?s=43&t=7eecH6cep1ONZ-NAMcRFBlw.

[36] Deng Cheng, Cyber Dragon: Inside China’s Information Warfare and Cyber Operations, 44-45.

[37] Tzu-chieh Hung and Tzu-wei Hung, “How China’s Cognitive Warfare Works : A Frontline Perspective of Taiwan’s Anti-Disinformation Wars,” 4.

[38] Paul Charon and Jean-Baptiste Jeangène Vilmer, “Chinese Influence Operations: A Machiavellian Moment,” IRSEM, 49-51; Nadine Yousif, “MP Michael Chong Urges US- Canada Cooperation on China Interference,” BBC News, 2023, https://www.bbc.com/news/world-us-canada-66791749.

[39] Emilio Iasiello, “China’s Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities,” Journal of Strategic Security 9, no. 2 (2016), 56.

[40] Aurel Sari, “Hybrid Threats and the Law: Concepts, Trends and Implications,” 2020, 10-12.; Bret Austin White, “Reordering the Law for a China World Order : China’s Legal Warfare Strategy in Outer Space and Cyberspace,” Journal of National Security Law & Policy 11, no. 2 (2021): 435-88.

[41] Charon and Jeangène Vilmer, “Chinese Influence Operations: A Machiavellian Moment,” 51-55.

[42] Pieter Zhao, “Chinese Political Warfare: A Strategic Tautology? The Three Warfares and the Centrality of Political Warfare within Chinese Strategy,” The Strategy Bridge, no. August (2023), https://thestrategybridge.org/the-bridge/2023/8/28/chinese-political-warfare-a-strategic-tautology.

[43] Rush Doshi and Robert D. Williams, “Is China Interfering in American Politics?,” Lawfare, no. October (2018).

[44] United Nations General Assembly, “Final Substantive Report,” Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 2021.

[45] See e.g. the so-called Martens Clause in the preamble of the 1899 Hague Convention of the Law and Customs of War on Land.

[46] Todd C. Helmus, “Artificial Intelligence, Deepfakes, and Disinformation: A Primer,” Rand Perspective, no. July (2022); Adrian Agenjo, “Lavender Unveiled : The Oblivion of Human Dignity in Israel’ s War Policy on Gaza,” Opinio Juris, no. April (2024): 1-5, http://opiniojuris.org/2024/04/12/lavender-unveiled-the-oblivion-of-human-dignity-in-israels-war-policy-on-gaza/.

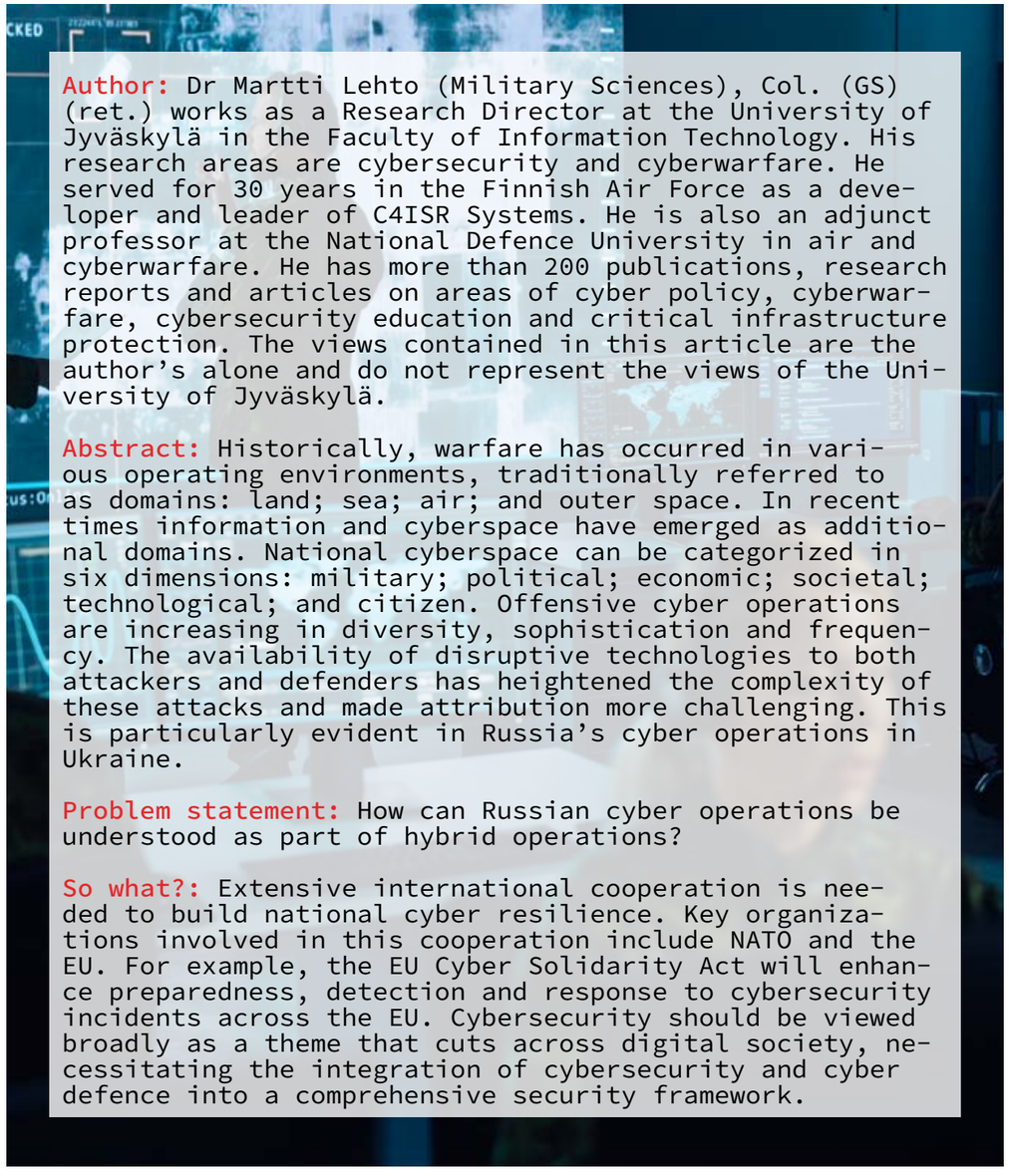
[47] Michael N. Schmitt, “Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations,” International Review of the Red Cross (Cambridge University Press, April 01, 2019).

[48] National Institute for South China Sea Studies, “A Legal Critique of the Award of the Arbitral Tribunal in the Matter of the South China Sea Arbitration,” Asian Yearbook of International Law 24 (2020).

[49] Soldatkin, Vladimir & Komuves, Anita, “Hungary‘s Orban talks Ukraine peace with Putin, stirring EU outcry,” Reuters, https://www.reuters.com/world/europe/hungarys-orban-says-no-position-negotiate-between-ukraine-russia-2024-07-05/.

National cyberspace and cyber operations

MARTTI LEHTO



Author: Dr Martti Lehto (Military Sciences), Col. (GS) (ret.) works as a Research Director at the University of Jyväskylä in the Faculty of Information Technology. His research areas are cybersecurity and cyberwarfare. He served for 30 years in the Finnish Air Force as a developer and leader of C4ISR Systems. He is also an adjunct professor at the National Defence University in air and cyberwarfare. He has more than 200 publications, research reports and articles on areas of cyber policy, cyberwarfare, cybersecurity education and critical infrastructure protection. The views contained in this article are the author's alone and do not represent the views of the University of Jyväskylä.

Abstract: Historically, warfare has occurred in various operating environments, traditionally referred to as domains: land; sea; air; and outer space. In recent times information and cyberspace have emerged as additional domains. National cyberspace can be categorized in six dimensions: military; political; economic; societal; technological; and citizen. Offensive cyber operations are increasing in diversity, sophistication and frequency. The availability of disruptive technologies to both attackers and defenders has heightened the complexity of these attacks and made attribution more challenging. This is particularly evident in Russia's cyber operations in Ukraine.

Problem statement: How can Russian cyber operations be understood as part of hybrid operations?

So what?: Extensive international cooperation is needed to build national cyber resilience. Key organizations involved in this cooperation include NATO and the EU. For example, the EU Cyber Solidarity Act will enhance preparedness, detection and response to cybersecurity incidents across the EU. Cybersecurity should be viewed broadly as a theme that cuts across digital society, necessitating the integration of cybersecurity and cyber defence into a comprehensive security framework.

The paradigm has changed, and the change continues

In the traditional warfare model, nation-states engage in conflict for various reasons tied to their national interests. Warfare is understood as occurring in the diverse domains or operational environments where military operations take place. These activities can be divided into kinetic actions with physical effects and non-kinetic actions.

The non-kinetic environment has evolved over the last 100 years, transitioning from radio to computer technology and Artificial Intelligence (AI). It comprises largely undetectable silent technologies capable of inflicting damaging, debilitating and degrading physical and neural effects on unwitting targets.[1]

Cognitive warfare involves understanding and influencing human perception, cognition and behaviour to achieve strategic objectives. Emerging technologies such as AI, especially generative AI, and neuro-technologies enable highly accessible and efficient subversion within the cognitive domain of warfare. The mass production of data and automated content creation have led to an abundance of publicly available data that can be used for cognitive manipulation. Consequently, data and AI algorithms have become weapons of cognitive warfare.[2]

Understanding national cyberspace

Cyber threats are complex and asymmetrical because digital cyberspace is borderless and multidimensional. The national cyber environment consists of various actors and functional entities. The cyber environment differs from the traditional national operating environment, where an independent state has clearly defined geographical boundaries - land, sea and airspace - that determine its jurisdiction.

Political dimension

The political dimension of national cyberspace represents the policy processes, legislative frameworks and regulations designed to promote, direct and control cybersecurity. The political nature of cyber issues is increasingly emphasized in both national and international politics. Cybersecurity issues are being presented more broadly and with greater significance in international fora and organizations such as the EU, NATO and the OSCE.

Like other diplomatic efforts, cyber diplomacy involves building strategic partnerships with countries globally to enhance collective action and cooperation against shared threats. This includes assembling coalitions of like-minded nations on vital policy issues, sharing information and national initiatives, and confronting bad actors. Cyber diplomacy employs diplomatic tools and initiatives to achieve objectives in cyberspace. Its goals include minimizing the consequences of cyber aggression such as cyber espionage and offensive cyber operations carried out by state or non-state actors. Additionally, it aims to address international law and norms in the field of cybersecurity and undertake actions that build trust. Mutual understanding and common rules can reduce the threat of various conflicts.[3]

The EU has produced several key frameworks and policies, including the Diplomatic Response Framework (Cyber Diplomacy Toolbox, 2017), the Cyber Defence Policy Framework (2018), the EU Cybersecurity Act (2019) and the Council Decision (2019) concerning restrictive measures against cyberattacks threatening the Union or its member states. Furthermore, following the EU's Cybersecurity Strategy for the Digital Decade, the bloc has introduced several acts and policy papers such as the NIS 2 Directive, the European Cyber Resilience Act, the Digital Operational Resilience Act, the European Cyber Defence Policy, the Strategic Compass of the European Union and the European Chips Act.[4]

Similarly, the EU Cyber Diplomacy Toolbox is a collective diplomatic response to malicious cyber activities. It is part of the EU's approach to cyber diplomacy within the Common Foreign and Security Policy. Its goal is to contribute to conflict prevention, mitigate cybersecurity threats and promote stability in international relations.[5]

Military dimension

As part of their military strategy, several nations are developing their capability of conducting operations in cyberspace, alongside land, sea, air and outer space. At the strategic level of cyberwarfare, one state aims to influence the vital functions of another. Cyber operations are integrated with other military forces at the operational and tactical levels.

NATO has long considered cyber defence a key component of its overall defence strategy. NATO's strong focus on cyber defence began at the 2002 NATO Summit in Prague. NATO and its allies are responding to cyber threats by enhancing their ability to detect, prevent and respond to malicious cyber activities. Strong and resilient cyber defences are crucial for NATO and its allies to fulfil the Alliance's three core tasks: deterrence and defence; crisis prevention and management; and cooperative security.[6]

At the 2023 NATO Summit in Vilnius member nations endorsed a new concept to enhance the contribution of cyber defence to NATO's overall deterrence and defence posture. They also launched NATO's Virtual Cyber Incident Support Capability (VCISC) to support national mitigation efforts in response to significant malicious cyber activities.[8]

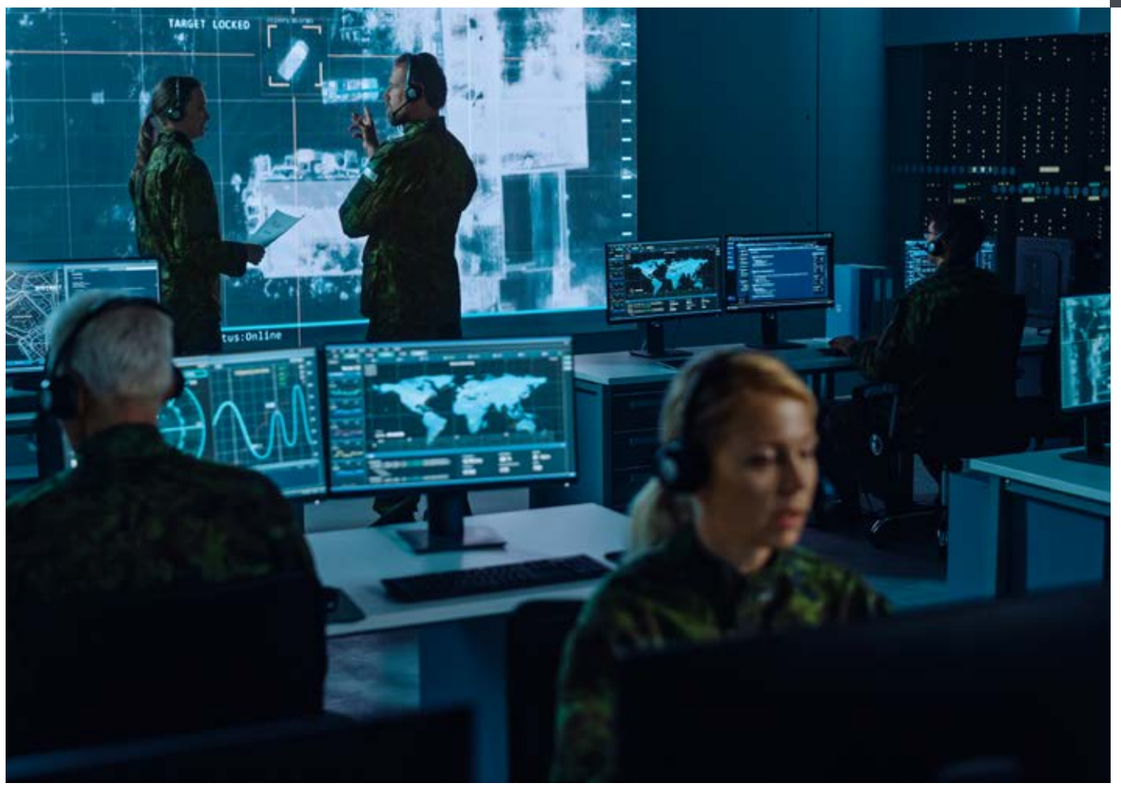
Defence forces need efficient cyber resilience, non-kinetic power convergence, and the capability of operating in and through contested and congested cyberspace. Two factors, cyber power and cyber deterrence, unite the military and political dimensions of cyberspace. The National Cyber Power Index describes a nation's ability to operate in a global cyber environment.[8] Cyberspace deterrence aims to influence an adversary's behaviour, discouraging them from engaging in unwanted activities.[9]

Societal dimension

The current decade of digitalization and data economy transformation is changing the world. This change affects us all, as digitalization and data are part of everyday life in every sector of society. This is reflected in new types of services, operating models, technologies and skill requirements. Digitalization covers virtually every area of welfare, including social services, the education sector and healthcare services.

The asymmetrical threat posed by cyberattacks and the inherent vulnerabilities of cyberspace constitute a serious security risk. In the cyber world one of the most important threats focuses on critical infrastructure (CI). CI includes the structures and functions vital to society's uninterrupted functioning, comprising both physical facilities and electronic functions and services such as political decision making, internal and external security, logistics, the economy, energy, telecommunications, and food production. In recent years, attacks against CI, critical information infrastructures and the internet have become increasingly frequent and complex as perpetrators have become more professional. Attackers can inflict damage on physical infrastructure by infiltrating the digital systems that control physical processes, damaging specialized equipment and disrupting vital services without a physical attack.[10]

A focus in the social dimension is Critical Infrastructure Protection (CIP), which involves actions taken to prevent and mitigate the risks resulting from the vulnerabilities of critical infrastructure assets and to facilitate recovery in the event of an attack.



Citizen dimension

Digital technologies have become deeply integrated into human life. The operational reliability of information and communications technology is essential for the smooth functioning of modern society, the security of its infrastructure and the wellbeing of its citizens. It is also crucial for maintaining public trust in societal operations. In a digital society citizens need to act safely and responsibly in the face of digital threats. Digitalization offers significant benefits, making life more efficient and enabling global communication. However, it also has impacts on citizens' private, social and public lives, influencing their privacy, autonomy and security.[11]

According to the EU Digital Compass, "Digital technologies should protect people's rights, support democracy, and ensure that all digital players act responsibly and safely. People should benefit from a fair online environment, be safeguarded against illegal and harmful content, and be empowered when interacting with new and evolving technologies like artificial intelligence. The digital environment should be safe and secure for all users, from childhood to old age, ensuring empowerment and protection."[12]

The digital skills targets set by the Digital Decade are still far from being achieved, with only 55.6 per cent of the EU population having at least basic digital skills. Member states are progressing towards the target of making all key public services and electronic health records accessible to citizens and businesses online, as well as providing them with secure electronic identification (eID). However, achieving 100 per cent coverage of digital public services for citizens and businesses by 2030 remains challenging.[13]

Economic dimension

Cybersecurity Ventures is a prominent industry research and media organiza-

tion recognized for its authoritative insights and contributions to cybersecurity. Based on its report, global cybercrime costs will increase by 15 per cent annually over the next five years, reaching USD 10.5 trillion per year by 2025. This would represent the largest transfer of economic wealth in history. Cybercrime costs encompass a range of issues, including damage to and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, disruption to normal business operations following an attack, forensic investigation, data and system restoration and deletion, and reputational damage.[14]

The global financial system depends increasingly on digital infrastructure. The economic impact of cyberattacks includes not only the direct costs to organizations but the long-term effects on national economies and the expenses related to enhancing cybersecurity at various levels. Preparing for cyberattacks can also influence taxation and public expenditure if additional resources are needed for cybersecurity in the public sector. Developing cybersecurity thus requires careful consideration from both economic and societal perspectives.[15]

Regulatory mechanisms can improve cybersecurity but also come with their own set of challenges. For example, preventive regulations, post-incident obligations and information access requirements provide various benefits and costs. The NIS 2 Directive is an example of such a regulatory approach because it provides legal measures to boost the overall level of cybersecurity in the EU. Political, societal and economic dimensions all play a role in achieving economic and financial stability. Effective public administration is crucial for maintaining democracy and ensuring societal welfare.

Technological dimension

Information and communications technology (ICT) encompasses a range of fields related to computer systems, software, hardware, and data processing and storage. One of the primary goals of ICT tools and systems is to enhance how individuals and organizations create, process and share data and information. ICT plays a crucial role in various areas, including business, education, healthcare, defence and leisure activities.[16]

Digital tools and software streamlining processes in business reduce manual operations and enhance online customer service. They enable businesses to automate tasks, improve efficiency and productivity, protect customer information, and build an information ecosystem. Digitalization also brings new threats, however. The cyber world attracts criminals seeking opportunities to steal, exploit and sell information. Cybersecurity solutions must be smart and effective to protect both citizens and organizations from these emerging threats.

Trust is a fundamental aspect of a digital society. Trust must be established and upheld for a digital society to fulfil its purpose and maintain social stability.

Cyber operations as part of hybrid operations

Hybrid operations incorporate several elements of cyber operations, aiming to remain below the threshold of armed conflict. Intentional instability can be maintained through cyber operations in both peacetime and wartime. Russia's hybrid warfare strategy can be described as a creative application of force that combines a broad spectrum of military and non-military tools and vectors of power across an extensive multidomain battlespace.

According to the NATO Washington Summit Declaration (2024), "Russia's full-scale invasion of Ukraine has shattered peace and stability in the Euro-Atlantic area and gravely undermined global security. Russia remains the most significant and direct threat to Allies' security."[17]

Political dimension

Russia is employing hybrid measures to influence the politics and policies of countries in the West and beyond. This strategy represents a significant challenge for Western governments. Russia aims to ensure that political outcomes in targeted countries are aligned with its national interests. Countries with weak legal and anti-corruption frameworks, or where domestic groups share Russia's interests or worldview, like Moldova, are particularly vulnerable. The Kremlin is capable of influencing elections and other political outcomes beyond its borders. The Russian theory of strategic culture explores and explains Russian offensive cyber operations such as cyberattacks and cyber espionage. Elements of Russian strategic culture related to these operations include asymmetric means of warfare and the denial, deception and concept of tactical truth. Russia's ongoing aggression in Ukraine highlights its continued threat to the rules-based international order. It is assumed that Russian offensive cyber capabilities are now being developed to achieve the same performance in these Western tactics, techniques and procedures.[18,19]

President Alexander Stubb of Finland has frequently addressed Russia's hybrid influence in his speeches, maintaining that Russia aims to destabilize societies through various forms of attack. He has also noted that modern conflicts often involve a mix of conventional and hybrid warfare and cyberwarfare, with hybrid attacks occurring frequently. In a speech at the Hertie School in Berlin on 8 May 2024, Stubb remarked, "Hybrid attacks are commonplace in peacetime, and they rarely come with a declaration of war. Traditional war is also complex and multifaceted. Conventional warfare still exists - as evidenced in both Europe and the Middle East - but the instruments and methods extend beyond mere shells and trenches."[20]

Military dimension

The use of cyber tools as a military strategy to target enemy forces and capabilities can be categorized similarly to other military operations. Cyber tools can be employed in conventional operations such as those observed in Ukraine or in more specialized operations like the Stuxnet attack against Iran. In these hybrid warfare operations methods are used to achieve specific objectives, often in a covert manner that, like special operations, falls below the threshold of traditional armed conflict. In war the objective of conflating kinetic tools and non-kinetic tactics is to optimally inflict paralysis and damage on an opponent's environment.[21]

Russia's invasion of Ukraine highlights the significant role cyber capabilities play in modern warfare, demonstrating how cyber tools can complement conventional military strategies. The Russian approach includes notable operations that have affected targets beyond Ukraine, as well as various aspects of Ukrainian infrastructure, government and civilian networks. The CyberPeace Institute has recorded 2,258 cyberattacks and operations, 666 of which were targeted at Ukraine, and 2,258 at other countries. These cyber incidents targeted 23 different critical infrastructure sectors, affecting Ukraine and some 49 other countries.[22]

At an event in Canada in June 2024 NATO Secretary General Jens Stoltenberg remarked: "The challenge is that we are threatened by something which is not a full-fledged military attack, which are these cyber, hybrid is below Article Five, as is often referred to, threats, and that is everything from meddling in our political processes, undermine the trust in our political institutions, disinformation, cyber-attacks, we have seen across Europe and how many sabotage actions against critical infrastructure, and so on."[23]

Societal dimension

The development of cybersecurity requires a focused long-term effort. Risks can materialize rapidly, and the operating environment is constantly evolving. In recent years attacks on critical infrastructure, including information systems and the internet, have become more frequent, complex and targeted as attackers have grown more professional. They can inflict damage on or cause disruptions to physical infrastructure by infiltrating digital systems that control physical processes, damaging specialized equipment and disrupting vital services without a physical attack. These threats continue to evolve in their complexity and sophistication.

Russia may target cyberattacks against critical infrastructure to create uncertainty and mistrust among citizens and demonstrate its capability of paralysing essential societal functions. Even as Russia focuses on cyber operations related to the Ukrainian conflict, it remains a persistent global cyber threat. For example, goals have been the telecommunications sector (Triolan and Vinasterisk ISP, Ukrtelecom, Kyivstar), broadcasting companies, media, transport and logistics providers, data centres, the energy sector, and border protection.[24,25,26]

Moscow uses cyber disruptions as a foreign policy tool to influence other countries' decisions. It is continuously refining its espionage, influence and attack capabilities against various targets. Russia can target critical infrastructure, including underwater cables and industrial control systems, both in the United States and in allied and partner countries. During 2024 Russia's cyberattack targets have:[27]

- focused on German political parties and German military officials;
- launched an espionage campaign against the embassies of Georgia, Poland, Ukraine and Iran and a ransomware attack against Sweden's digital service provider for government services;
- hacked Microsoft corporate systems and 65 Australian government departments and agencies, stealing 2.5 million documents in Australia's largest government cyberattack; and
- hacked residential webcams in Kyiv to gather information about the city's air defence systems before launching a missile attack on Kyiv.

Citizen dimension

The citizen dimension emphasizes the impact of information. Attackers can systematically spread disinformation through targeted social media campaigns to radicalize individuals, destabilize society and control the political narrative.

Russia's disinformation and propaganda ecosystem encompasses various official communication channels, social media, proxy sources and unattributed platforms used to create and amplify false narratives. This ecosystem consists of five main pillars: official government communications; state-funded global messaging; the cultivation of proxy sources; the weaponization of social media; and cyber-enabled disinformation. The Kremlin employs these tactics and platforms as part of its strategy of weaponizing information. Such disinformation and propaganda organizations include:[28,29]

- The Strategic Culture Foundation, an online journal registered in Russia directed by Russia's Foreign Intelligence Service (SVR);
- Global Research, a Canadian website that is part of Russia's disinformation and propaganda ecosystem;
- New Eastern Outlook, a pseudo-academic publication of the Russian Academy of Science's Institute of Oriental Studies that promotes disinformation and propaganda focusing primarily on the Middle East, Asia and Africa;
- News Front, a Crimea-based disinformation and propaganda organization providing an "alternative source of information" for Western audiences;
- SouthFront, a multilingual online disinformation site registered in Russia that focuses on military and security issues;
- Katehon, a Moscow-based quasi-think tank focusing on anti-Western disinformation and propaganda; and
- Geopolitica.ru, a platform for Russian ultranationalists that spreads disinformation and propaganda targeting Western audiences.

Economic dimension

Without dedicated action the global financial system will become increasingly vulnerable as innovations, competition and disruptive technologies continue to drive the digital revolution. While many threat actors are motivated by financial gain, a growing number of state-sponsored attackers are also launching disruptive and destructive attacks against financial systems.

Cybersecurity is crucial for maintaining economic and financial stability. For example, Russia seeks to influence European politics both directly and indirectly and has used energy as a tool of foreign policy. Cyber operations targeting critical infrastructure and economic systems can further destabilize economic and financial stability. As an MP, Rishi Sunak analysed possible Russian hybrid attacks in December 2017, saying, "Sabotage of undersea cable infrastructure is an existential threat to the UK. The result would be to damage commerce and disrupt government-to-government communications, potentially leading to economic turmoil and civil disorder."[30,31]

The effective protection of the global financial system is primarily an organizational challenge. While efforts to strengthen defences and tighten regulations are important, they are insufficient to keep pace with the growing risks. Unlike many sectors, the financial services community generally has the necessary resources and technical capabilities. The key challenge is to coordinate cybersecurity protection across governments, the financial authorities and industry, as well as to leverage existing resources effectively and efficiently.[32]

Technological dimension

An attack vector is a path or means by which an attacker can gain unauthorized access to a computer, network or IT/OT infrastructure to deliver a payload or malicious action. Attack vectors allow attackers to exploit system vulnerabilities.[33]

Between December 2021 and March 2022 US CYBERCOM's joint forces, in close cooperation with the government of Ukraine, conducted defensive cyber operations alongside Ukrainian Cyber Command personnel. This effort was part of a broader initiative to enhance cyber resilience in critical national networks. The teams implemented a threat-hunting operation in Ukraine, as well as remote analytic and advisory support, using innovative techniques. They also conducted network defence activities aligned to critical networks. They identified 90 instances of malicious code the Russians had created to disrupt Ukrainian infrastructure. The teams also gained a valuable insight into adversaries' tactics, techniques, procedures, plans, capabilities and tools.[34]

Russian cyber threat activity against Ukraine has been carried out by various actors associated with the three main Russian security services: the Federal Security Service (FSB); the Foreign Intelligence Service (SVR); and the Main Intelligence Directorate (GRU). These cyber actors have engaged in various threat activities against Ukraine, including disruptive and destructive cyber operations.

Prosecutors at the International Criminal Court (ICC) are investigating alleged Russian cyberattacks on Ukrainian civilian infrastructure as possible war crimes. ICC prosecutors are working with Ukrainian teams to investigate attacks that endangered lives by disrupting power and water supplies, cutting connections to emergency responders, or disabling mobile data services that transmit air raid warnings.[35]

Towards cognitive warfare

Hybrid threats aim to exploit a country's vulnerabilities and often seek to undermine fundamental democratic values and liberties. The digital cyber world can be divided into six interacting dimensions, with human beings at the core of each. In these dimensions people act as politicians, decision makers, operators, soldiers, developers, citizens and more. Cognitive superiority and cognitive warfare permeate all these dimensions, indicating a shift from purely kinetic approaches towards subversion.

The internet and social media are today among the most powerful tools in cognitive warfare, targeting key figures, niche groups and the public. Social media platforms have become crucial battlegrounds, influencing and manipulating public perceptions, opinions and behaviours. Artificial intelligence has the potential to revolutionize cognitive warfare by enabling more sophisticated and effective strategies.

Nations should counter hybrid influence, especially in the cyber environment. States should ensure that activities in cyberspace and national policies are designed and implemented to support a comprehensive and systemic approach to cybersecurity and cyber defence. They should improve dialogue, cooperation and information exchange about national, regional and global cybersecurity. Building societal resilience against hybrid threats and cognitive warfare operations requires cooperation between all relevant civil society organizations, the private sector, academic communities and NGOs. Finally, extensive and interdisciplinary research, education and training are needed in cyberspace and the cognitive environment.

Endnotes

[1] Martti Lehto and Gerhard Henselmann, "Non-kinetic Warfare: The new game changer in the battle space," 15th International Conference on Cyber Warfare and Security, 2020, Old Dominion University, Norfolk, Virginia, USA, 316-325.

[2] Alonso Bernal, Cameron Carter, Ishpreet Singh, Kathy Cao, and Olivia Madreperla, "Cognitive warfare: An attack on truth and thought," NATO and Johns Hopkins University report, Fall 2020.

[3] EU parliament, "Insights, Understanding the EU's approach to cyber diplomacy and cyber defence," European Union, May 28, 2020, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)651937.

[4] Annegret Bendiek and Matthias C. Kettemann, "Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy," SWP comment, no. 16, February 24, 2021, https://www.swp-berlin.org/10.18449/2021C16/.

[5] Cyber Risk GmbH, "The Cyber Diplomacy Toolbox," https://www.cyber-diplomacy-toolbox.com/.

[6] NATO Cyber Defence, Factsheet, April 2021, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf.

[7] NATO, "Cyber defence," last updated: September 14, 2023, https://www.nato.int/cps/en/natohq/topics_78170.htm.'

[8] Julia Voo, Irfan Hemani, and Daniel Cassidy, "National Cyber Power Index 2022," Harvard Kennedy School, Belfer Centre Report, September 2022, https://www.belfercenter.org/publication/national-cyber-power-index-2022.

[9] Chris Jaikaran, "Cybersecurity: Deterrence Policy," January 18, 2022, https://crsreports.congress.gov/product/pdf/R/R47011.

[10] Martti Lehto, "Cyber-attacks Against Critical Infrastructure," in: Cyber Security: Critical Infrastructure Protection, in Computation Methods in Applied Sciences series, ed. M Lehto and P Neittaanmäki (Springer 2022), 3-42, ISBN: 978-3-030-91293-2.

[11] Anne Gardenier, Rinie van Est, and Lambèr Royakkers, "Technological Citizenship in Times of Digitization: An Integrative Framework," Digital Society, Volume 3, Issue 2: 21 (2024), https://doi.org/10.1007/s44206-024-00106-1.

[12] EU, "Europe's Digital Decade: Digital targets for 2030," https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.

[13] European Commission, "Second report on the State of the Digital Decade calls for strengthened collective action to propel the EU's digital transformation," July 02, 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3602.

[14] Steve Morgan, "Cybercrime to Cost the World $10.5 Trillion Annually by 2025" (Special Report, November 13, 2020), Cybercrime Magazine, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[15] ENISA, "Cybersecurity as an Economic Enabler," March 2016, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler.

[16] Martti Lehto, "Cyber-attacks Against Critical Infrastructure," in: Cyber Security: Critical Infrastructure Protection, in Computation Methods in Applied Sciences series, ed. M. Lehto and P. Neittaanmäki (Springer 2022), 3-42, ISBN: 978-3-030-91293-2.

[17] NATO, https://www.nato.int/cps/en/natohq/official_texts_227678.htm.

[18] Arsalan Bilal, "Russia's hybrid war against the West," NATO Review, April 26, 2024, https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html.

[19] Martti J. Kari, "Russian Strategic Culture in Cyberspace," JYU Dissertations 122, October 11, 2019.

[20] Alexander Stubb, "Comprehensive Security in the 21st century: The Finnish model," May 08, 2024, https://www.presidentti.fi/en/speech-by-president-of-the-republic-of-finland-alexander-stubb-at-hertie-school-in-berlin-on-8-may-2024/.

[21] Arsalan Bilal, "Hybrid Warfare: New Threats, Complexity, and "Trust" as the Antidote," NATO Review, November 30, 2021, https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

[22] Stéphane Duguin and Pavlina Pavlova, "The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict," EU Directorate-General for External Policies Policy Department, Workshop September 2023, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf.

[23] NATO, "Speech by NATO Secretary General Jens Stoltenberg at event hosted by the NATO Association of Canada and the Canadian NATO Parliamentary Association," June 19, 2024, https://www.nato.int/cps/en/natohq/opinions_226837.htm.

[24] ODNI, "Annual Threat Assessment of the U.S. Intelligence Community," February 05, 2024, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

[25] Stéphane Duguin and Pavlina Pavlova, "The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict," EU Directorate-General for External Policies Policy Department, Workshop September 2023, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf.

[26] CyberPeace Institute, https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline.

[27] CSIS, "Significant Cyber Incidents," https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[28] DoS, "GEC Special Report: August 2020 Pillars of Russia's Disinformation and Propaganda Ecosystem," August 2020.

[29] Government of Canada, "Russia's use of disinformation and information manipulation," February 28, 2024, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=eng.

[30] NATO STRATCOM COE, "Russia's Strategy in Cyberspace," June 2021.

[31] Helmi Pillai, "Protecting Europe's critical infrastructure from Russian hybrid threats" (Centre for European Reform, Policy Brief, April 25, 2023), https://mailings.cer.eu/publications/archive/policy-brief/2023/protecting-europes-critical-infrastructure-russian-hybrid#FN-25.

[32] Tim Maurer and Arthur Nelson, "The Global Cyber Threat" (IMF report, Spring 2021), https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm.

[33] Martti Lehto, "Cyber-attacks against Critical Infrastructure," in: Cyber Security: Critical Infrastructure Protection, in Computation Methods in Applied Sciences series, ed. M. Lehto and P. Neittaanmäki (Springer 2022), 3-42, ISBN: 978-3-030-91293-2.

[34] Cyber National Mission Force, "Before the Invasion: Hunt Forward Operations in Ukraine," November 28, 2022, https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/.

[35] Anthony Deutsch, Stephanie van den Berg and James Pearson, "ICC probes cyberattacks in Ukraine as possible war crimes," June 14, 2024, https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14/.

Defending Free Speech With Free Choice:

Towards Technology-Driven, Human-Centred, Endpoint Solutions For Society As A Whole

MARIA PAPADAKI

Author: Dr. Maria Papadaki is an Associate Professor in Cyber Security at the University of Derby, UK. Her research interests focus on incident response, threat intelligence, maritime cyber security, and human-centred security. Her research outputs include 70+ international peer-reviewed publications in this area. The views contained in this article are the author's alone and do not represent the views of the University of Derby.

Abstract: Cognitive warfare and, particularly, disinformation, is now heavily reliant on social media platforms, cybertechnologies, and AI, with the aim to cause confusion, societal polarisation, mistrust, anger, and hatred against governments, organisations, communities, or opposing individuals. While disinformation is a global problem, early defences based on censorship also threaten core Western values, such as freedom of speech and democracy. Unsurprisingly, surveyed EU citizens overwhelmingly consider disinformation as a threat to democracy.

Problem statement: How can cybersecurity and AI serve democratic values and human rights for cognitive threats support, while seeking to introduce the need for transparent, customisable, cognitive endpoint support tools?

So what?: The need to complement existing defences at endpoints is analysed, and indicative functionality is outlined and grouped according to the different response objectives, namely support and education, threat surface reduction, detection and response, and situational awareness. A conceptual architecture, requirements analysis, use cases, and proof-of-concept functionality could extend this work to illustrate its key points.

The Rise of Social Media and Demagogues

The rise of demagogues through democracy is not a new phenomenon, nor are their attempts to exploit new communication media to spread propaganda, manipulate the public, and eventually lead them to tyranny. Ever since the inception of democracy, Plato warned of the danger of demagogues using democracy's freedoms against itself. In modern times, social media, as a new communication medium, invites many parallels to be drawn from historical examples, albeit now with global reach and amplified consequences.

While studies agree that mainstream media, such as newspapers, radio, and television, remains the most important communication platforms, they also acknowledge the growing popularity of social media as a news and media outlet, especially among younger demographics. As the Flash Eurobarometer 536 survey reveals, a quarter of EU citizens have found data and statistics about their country or Europe on social media, particularly ones among the 15-24 age group.[1] Similarly, almost 2 in 5 respondents to the 2023 Media & News Survey (and 3 in 5 15-24-year-olds) used social media to access news.[2] The percentage is even higher in the UK, with almost half of UK adult respondents and 71% of 16-24-year-olds using social media for news.[3] Notably, the rise of TikTok as a news media platform is steep, with 10% of 16-plus year-olds receiving news through it in 2023, up from 1% in 2020.[4]

Therefore, it is understandable that political parties, organisations, and individuals use social media to reach their audiences. However, un-

like mainstream media, where the same content is transparently available to all who choose to access it, social media content is curated, microtargeted, promoted or suppressed by opaque platform algorithms, often irrespective of user choice.[5] This limits accountability and opens the door for demagogues who seek to manipulate and polarise through disinformation. Despite the challenges of auditing, disinformation tracking software, such as that developed by researchers at Trollrensics, has been developed. It found coordinated networks used to flood social networks with disinformation during the 2024 European elections, particularly in the interests of far-right parties. Analysis of 2.3 million posts in France, Germany, Italy, and the Netherlands revealed 50,000 accounts spreading disinformation; 1 in 5 posts mentioned far-right French politician Éric Zemmour, and 1 in 10 German posts about Alternative für Deutschland party, came from disinformation accounts.[6] With three billion people across the world expected to vote in elections in 2024 and 2025, it is perhaps no surprise that disinformation was identified by the World Economic Forum (WEF) as the most severe global risk over the next two years. WEF also confirms the strong links between disinformation and societal and political polarisation, interstate violence, and erosion of human rights.[7] Democracy and human rights (including free speech) are particularly important values to Western societies.[8]

From Disinformation to Polarisation and Cognitive Warfare

In addition to attempting to sway elections in favour of autocratic candidates, the broader role of disinformation in cognitive warfare should be considered. Professor Miller recognises disinformation and sophisticated psychological manipulation techniques as key features of cognitive warfare.[9] Heavily reliant on social media platforms, cybertechnologies, and AI. These techniques remain closely interlinked and aim to cause confusion, societal polarisation, mistrust, anger, and hatred towards Western governments, organisations, communities, or opposing individuals.[10, 11] The war in Ukraine has provided ample examples of the role of disinformation/FIMI in cognitive warfare, and how Ukrainian forces have adapted their defences accordingly.[12]

Arguably, allowing these threats to proliferate could lead to the rise of extremist, far-right, and misogynistic movements, which could threaten human rights. Some early indications can be seen in a study by King‘s College London and Ipsos, which showed that younger male participants expressed more negative views towards feminism than their older counterparts.[13] Andrew Kaung, a former TikTok analyst, revealed the differences in content recommendations that teenage girls and boys would receive, irrespective of their choices. Teenage boys would be shown violent, misogynistic content, while girls would be shown content on music or make-up.[14] A further study by NPCC has indicated a notable rise in the number of crimes against women and girls in the UK, which may be linked to the radicalisation of men by social media influencers promoting misogyny. As a result, they have since upgraded gender-based crimes to a national threat, akin to organised crime and terrorism.[15]

An example of disinformation fuelling violence and extremism can be observed after the killing of three children in Southport, UK, in July 2024. Despite the UK authorities publishing the details of the suspect, who was born in the UK, the crime had already been attributed to immigrants through disinformation from foreign-owned websites. The false association between immigration and violent crime has had the unfortunate effect of mobilising far-right groups, which resorted to attacking immigration support structures across the country. There was a particular focus on Muslim and refugee communities, which led to attempts to incite anger, violence, anxiety, and fear across society.[16, 17] It would be premature to attribute this disinformation incident to FIMI actors at the time of writing. Nevertheless, despite any intent or attribution, its effects were real, and this relationship should be acknowledged.

The 2nd EEAS report on FIMI Threats offers an updated overview of the FIMI ecosystem and reveals its global scale and diverse range of targets. Nearly half of the analysed cases targeted countries across the globe, 30% targeted organisations (such as the EU, NATO, and Euronews), and nearly 20% of cases targeted individuals, including non-political figures. Furthermore, there seems to be an emerging trend of gender-based and anti-LGBTIQ+ FIMI attacks.[18]

It would be remiss not to consider the potential implications of AI-generated fake content, which WEF identified as a significant risk for 2024.[19] It is worth noting that AI-generated audio imitating the voices of politicians has already been utilised in a limited capacity in FIMI cases.[20] The relatively low technological barrier to creating fake content, coupled with the speed and volume at which it can reach individuals, suggests potential for concern. Notable examples illustrating its impact, besides character assassination, would be deepfake pornography and stock market manipulation. For example, explicit deepfake images of U.S. singer Taylor Swift reached millions of views before eventually being removed. Similarly, the promotion of a deepfake image featuring a Pentagon explosion ended up affecting U.S. stock markets before U.S. authorities countered the rumours.[21]

It is possible that this climate of intimidation, polarisation and violence, with FIMI in a featured role, could also lead to self-censorship, apathy, or coercion if people fear the unwanted consequences of defamation or violence by speaking up. The 2023 Freedom of the Net report indicates that there have been a significant number of attacks against free speech.[22] In three-quarters of the countries surveyed, individuals have faced legal repercussions for expressing themselves online. In four out of seven countries, this has even resulted in physical assault or even loss of life.

Censorship vs Free Choice

Autocratic regimes have been known to resort to conventional and AI-powered censorship to control the narrative. This can manifest in several ways, including blocking dissenting political, religious, or social content, the repression of free speech, and the gradual yet consistent divergence from international human rights conventions.[23] However, censorship could not work in Western societies without eventually opposing their core values and freedoms. WEF flags the risk that some governments will act too slowly, considering the trade-off between preventing disinformation and protecting free speech. In contrast, others may erode human rights and increase censorship by adopting authoritarian practices.[24]

EU citizens also recognise these risks and overwhelmingly consider disinformation a threat to democracy.[25] Considerable work is underway to gain a deeper understanding of cognitive warfare and develop collaborative, multilevel defences.[26, 27] A noteworthy and comprehensive response framework for FIMI threats is the FIMI Toolbox, which is based on a multilevel, collaborative, multidisciplinary, whole-of-society approach.[28]

When considering who has the right and the responsibility to decide on the level of protection, there are several stakeholders, each with distinct responsibilities. While it is within the authorities‘ power to define, regulate and block patterns of illegal activity, there is still scope for further protection, which could fall under the responsibility of individual citizens, should they choose to utilise them.

User Susceptibility to Fake Stories

Maertens et al. designed the Misinformation Susceptibility Test (MIST) to understand the scale of human error in identifying fake stories.[29] After surveying approximately 1,500 U.S. citizens, it was found that two out of three news stories could be correctly identified. However, younger adults and those relying on social media for their news were less successful.[30] Meanwhile, the Eurobarometer survey, conducted in the EU, indicates that 30% of surveyed EU citizens are not confident in recognising disinformation. Confidence level decreases with age and increases with the level of education.[31] A UK-based Ofcom survey reported similar levels of uncertainty, where 1 in 3 UK internet users were found to be unsure or unaware of the truthfulness of online information. It is also worth noting that a small subset, 6%, even believed everything online was unquestionably true.[32] It would be fair to say that the error or uncertainty levels are high, particularly when considering the error rates of another human-related threat, phishing. While not directly comparable threats or studies, the 2024 Verizon Data Breach Investigations report might still be worth considering, which suggests that phishing click rates ranged from 3-10% over the past eight years.[33]

To reduce error rates, it might be helpful to consider the potential impact that education could have. In the case of phishing, Spitzner empirically suggests that initial click rates at the outset of an organisation‘s journey towards raising awareness could typically range between 25 and 30 per cent before eventually dropping to less than 5 per cent within 18 to 22 months.[34] Awareness and education could highlight cognitive biases and emotional manipulation, and encourage critical thinking, allowing humans to spot warning signs of unusual, unexpected attacks. It is also worth acknowledging the wider range of complementary multilayer technological approaches that could contribute to reducing the threat space through automation and, ultimately, the likelihood of human error by encouraging users to adhere to security norms. These could include email content filtering, blacklisting of known accounts, email origin authentication and validation (in the form of DMARC, DKIM, and SPF).

Returning to FIMI and disinformation, it would be useful to consider how AI and human-centric security could help to reduce the likelihood of human error (assuming user consent is present). This could involve reducing the threat space, the cognitive load of distinguishing the legitimacy or authenticity of stories, and the technological gap between humans and technological controls.

Disinformation Detection

As a preliminary step towards reducing human error and maximising user support, this section explores disinformation detection approaches, including sentiment analysis, propagation pattern analysis, origin reputation, provenance, deepfake detection, confirmation bias user profiling, and fact-checking. This represents a selection of approaches that have informed the options presented in this article, rather than an exhaustive list.

Early approaches focused on signs of emotionally charged, manipulative language or discourse patterns featured in news stories and social media reactions. These approaches involved natural language processing and sentiment analysis of social network content, particularly on X/Twitter.[35]

A prominent indicator worthy of our attention is how these stories spread. Investigations showed that stories aiming to evoke strong reactions are likely to spread faster, or at least differently, than genuine news. One further advantage of identifying anomalous propagation patterns is that it is content-agnostic, which makes it more easily applicable to multilingual environments. Graph neural networks, or temporal graph networks, can be particularly effective at indicating signs of rapidly growing news stories, even adjusting to evolving propagation patterns.[36, 37]

Similarly, it might be possible to identify the anomalous behaviour of bot accounts spreading disinformation as a basis for informing their reputation. Initiatives, such as the Coalition for Content Provenance and Authenticity (C2PA), could go even further by cryptographically signing media content to verify its source and editing history. The presence of provenance information, or even the lack of it, could help to improve trust in the authenticity and origin of image, audio, or video content.[38]

Deepfake detection aims to identify anomalous effects caused by the editing processes of AI-generated software. In deepfake videos, such inconsistencies may be observed in movement or misalignments of key facial points, in unusual lighting, shadows, and reflections, both within individual frames and sequences of frames. Various methods can be used for detecting deepfakes, with deep learning, and multimodal deep learning approaches proving particularly effective.[39]

Another indicator considers the possibility that an individual may be more likely to believe and spread misinformation if it already aligns with their existing beliefs, a phenomenon known as confirmation bias. Therefore, user behaviour profiles of their historical usage could help to predict individuals who could unwittingly spread misinformation.[40]

The techniques mentioned above are designed to detect various patterns of anomalous activity of different entities, which can demonstrate that disinformation detection is indeed possible. There is potential for further improvement by combining these techniques, or even by complementing them with mapping wider characteristics of FIMI and cyber incidents, as defined in the DISARM and ATT&CK frameworks, respectively.[41]

Last but not least, it is important to consider the powerful potential of computer-human teaming methods in the context of fact-checking. Communities worldwide collaborate to investigate the accuracy of information based on journalistic standards and unpack the narrative, intent, and potential impact behind disinformation.[42] The emerging field of Large Language Models (LLMs) and generative AI, which have been trained on disinformation datasets, incorporate fact-checking functionality. These are also important and particularly relevant to end users. While LLMs show great promise, it would be prudent to await further evidence of their accuracy and resilience against disinformation attacks.

Towards Endpoint Solutions for FIMI Threats

While cybersecurity principles have inspired the FIMI Toolbox, it is important to acknowledge its stronger socio-cognitive elements that extend beyond technical aspects to encompass a broader range of societal considerations. Its collective response protocols involve an extensive network of relevant stakeholders across society, each with distinct responsibilities, ensuring proportional, adaptive, collective, understandable, and effective responses.[43]

Users and citizens have roles and responsibilities as stakeholders to protect their information space and explore how a response paradigm could be provided in a way that is transparent and democratic. To this end, it is suggested that protection, detection, and support functionality is made available at endpoints, where users can freely decide which ones to enable with the support of customisable default settings. Such user-centric functionality would provide the capacity for the greatest possible support, minimise the risk of human error, and accompany each option with the freedom to enable or disable it

at the user level. A group of indicative options for users are outlined below: support and education, threat surface reduction, detection and response, and situational awareness.

Support and Education

User-initiated support that facilitates the use of fact-checking, credibility/reputation scoring, bot detection, disinformation tracking, and education could be made available to users through browser extensions, context menu options, or LLMs. For instance, deepfake audio and video verification functionality (akin to solutions such as Microsoft Video Authenticator, Resemble AI, Sensity AI, or WeVerify) could be invoked to verify the credibility of deepfake audio or videos. Simplified reports for fact-checking, reverse image search, and content verification could also prove useful. Additionally, access to educational training resources could be facilitated, to help users recognise warning signs of disinformation, and emotional manipulation, operate suitable tools, understand their output, and select suitable, proportionate response options. Support functionality could also facilitate access to disinformation resources and communities for users who wish to volunteer, connect, or report suspected threats.[44]

Threat Surface Reduction

Options for reducing the threat surface could include automated countermeasures for known threats that users would prefer not to see regularly. Several countermeasures could potentially be employed, such as highlighting flagged content, filtering it, replacing it with its authentic alternative, or saving it to a secondary alternative location for future review (similar to spam folders for suspected junk email). For instance, the default setting might be configured to automatically filter content associated with known disinformation accounts. However, a user might also filter out deepfake political content or content featuring violence and extremism. Another user might want to redirect political content that lacks verified origin to a secondary location for later review. To avoid undue technological barriers, customisable default recommended settings and user-friendly interfaces that encourage proportionate and appropriate threat reduction would be beneficial, regardless of the social media applications used.

Detection and Response

The detection functionality could focus on identifying residual activity and more subtle warning signs of novel disinformation threats. Such instances could be reported to the user, escalated to human-computer teams for analysis, or logged locally for future investigation. For example, it might be possible to identify users who are prone to unwittingly forwarding misinformation to others. A user activity report highlighting the misinformation might lead to useful prompts and guidance to relevant educational content.

Situational Awareness

It may be beneficial to exchange threat intelligence information that aids situational awareness and helps to link events with other domains. Post-incident review of user settings could also fall under this functionality group.

Conclusions and Future Work

The considerable concern about disinformation, the importance of democratic values, and the degree of uncertainty expressed by users in their ability to correctly identify disinformation suggests the need for strengthening protection at endpoints and indicates that users might be willing to adopt the proposed functionality. The technological gap or privacy concerns might prove to be barriers for some people. Generative AI can prove particularly helpful in bridging technological gaps in user support, as would the use of optimal default profile settings. Raising awareness of privacy-enhancing technologies could alleviate fears and assure privacy protection.

Privacy-enhancing technologies, such as differential privacy and federated learning, among others, could enable the utility of relevant data while assuring its privacy in accordance with data protection principles. This is particularly important for supporting detection and response, situational awareness, or user profiling, where the privacy requirements would be higher. Since the focus is on examining content rather than user behaviour, it could be argued that the privacy requirements of support, education, and threat space reduction functionality would be relatively lower. In any case, the privacy requirements of any endpoint functionality must be determined and justified prior to seeking user consent.

The proposed endpoint functionality aims to complement existing defences and social media controls by democratising protection. It seeks to empower users with the right and responsibility to control their own information space, irrespective of their social media applications, encouraging transparency. It aims to bridge the technological gap between humans and disinformation controls, maximise support, reduce the likelihood of human error, and promote secure behaviour as the norm. Additionally, it strives to offer freedom of choice to individuals in cases where centralised controls could risk eroding democratic values and human rights. A conceptual architecture, requirements analysis, use cases, and proof of concept functionality could extend this work in the future to illustrate its key points.

Endnotes

[1] European Commission, “Flash Eurobarometer 536 Report: Public awareness and trust in European statistics,” February 2024, https://europa.eu/eurobarometer/surveys/detail/2955.

[2] European Parliament, “Media & News Survey 2023,” November 2023, https://europa.eu/eurobarometer/surveys/detail/3153.

[3] OFCOM, “News consumption in the UK: 2023, Research findings,” July 2023, https://www.ofcom.org.uk/media-use-and-attitudes/attitudes-to-news/news-consumption/.

[4] Idem.

[5] Urbano Reviglio, and Claudio Agosti, “Thinking Outside the Black-Box: The Case for “Algorithmic Sovereignty” in Social Media,” Social Media + Society 6, no. 2 (April 2020), https://doi.org/10.1177/2056305120915613.

[6] Lisa O'Carroll, “Disinformation networks ‘flooded’ X before EU elections, report says,” July 2024, https://www.theguardian.com/world/article/2024/jul/12/disinformation-networks-social-media-x-france-germany-italy-eu-elections.

[7] World Economic Forum, “The Global Risks Report 2023: 18th Edition Insight Report,” January 2023, https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

[8] European Parliament, “Eurobarometer: Parlemeter 2022,” January 2023, European Commission, "Flash Eurobarometer 536 Report: Public awareness and trust in European statistics," February 2024, https://europa.eu/eurobarometer/surveys/detail/2955.

[9] Seumas Miller, “Cognitive warfare: an ethical analysis,” Ethics Inf Technol 25, 46 (September 2023), https://doi.org/10.1007/s10676-023-09717-7.

[10] Nicolas Hénin, “FIMI: Towards a European redefinition of Foreign Interference,” EU Disinfo Lab, April 2023, https://www.disinfo.eu/publications/fimi-towards-a-european-redefinition-of-foreign-interference/.

[11] Erika Magonara, Apostolos Malatras, “Foreign Information Manipulation and Interference (FIMI) and Cybersecurity - Threat Landscape,” ENISA, December 2022, https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape/.

[12] Jakub Kalenský and Roman Osadchuk, “How Ukraine fights Russian disinformation: Beehive vs mammoth,” Hybrid CoE Research Report 11, January 2024.

[13] King’s College London and Ipsos, “Emerging tensions? How younger generations are dividing on masculinity and gender equality,” February 2024, https://www.kcl.ac.uk/policy-institute/assets/emerging-tensions.pdf.

[14] Marianna Spring, “'It stains your brain': How social media algorithms show violence to boys,” BBC Panorama, September 2024, https://www.bbc.co.uk/news/articles/c4gdqzxypdzo.

[15] NPCC, “Violence Against Women and Girls (VAWG): National Policing Statement 2024,” July 2024, https://cdn.prgloo.com/media/5fc31202dd7e411ba40d29fdca7836fd.pdf.

[16] Mark Easton, “Protests reveal deep-rooted anger, but UK is not at boiling point,” August 2024, https://www.bbc.co.uk/news/articles/czx66dkx3wlo.

[17] Marianna Spring, “Did social media fan the flames of riot in Southport?,” July 2024, https://www.bbc.co.uk/news/articles/cd1e8d7llg9o.

[18] European External Action Service (EEAS), “2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A framework for networked defence,” January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf.

[19] World Economic Forum, “The Global Risks Report 2023: 18th Edition Insight Report,” January 2023, https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

[20] European External Action Service (EEAS), “2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A framework for networked defence,” January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf.

[21] Luke Hurst, “ How a fake image of a Pentagon explosion shared on Twitter caused a real dip on Wall Street,” Euronews, May 2023, https://www.euronews.com/next/2023/05/23/fake-news-about-an-explosion-at-the-pentagon-spreads-on-verified-accounts-on-twitter.

[22] Shahbaz, Funk, and Vesteinsson, “The Repressive Power of Artificial Intelligence,” in: Shahbaz, Funk, Vesteinsson, Brody, Baker, Grothe, Barak, Masinsin, Modi, Sutterlin eds. Freedom on the Net 2023, Freedom House, 2023, freedomonthenet.org.

[23] Idem.

[24] World Economic Forum, “The Global Risks Report 2023: 18th Edition Insight Report,” January 2023, https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

[25] European Commission, “Flash Eurobarometer 464: Fake news and disinformation online,” April 2018, https://europa.eu/eurobarometer/surveys/detail/2183.

[26] European External Action Service (EEAS), “2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A framework for networked defence,” January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf.

[27] European External Action Service (EEAS), “1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence,” February 2023, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023.pdf.

[28] European External Action Service (EEAS), “2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A framework for networked defence,” January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf.

[29] Rakoen Maertens, Friedrich M. Götz, Hudson F. Golino, Jon Roozenbeek, Claudia R. Schneider, Yara Kyrychenko, John R. Kerr, Stefan Stieger, William P. McClanahan, Karly Drabot, James He, and Sander van der Linden, 2024, “The Misinformation Susceptibility Test (MIST): A psychometrically validated measure of news veracity discernment,” Behaviour Research Methods 56, 1863–1899 (March 2024), https://doi.org/10.3758/s13428-023-02124-2.

[30] Linley Sanders, “How well can Americans distinguish real news headlines from fake ones?,” June 2023, https://today.yougov.com/politics/articles/45855-americans-distinguish-real-fake-news-headline-poll.

[31] European Parliament, “Media & News Survey 2022,” July 2022, https://europa.eu/eurobarometer/surveys/detail/2832.

[32] OFCOM, “The genuine article? One in three internet users fail to question misinformation,” March 2023, https://www.ofcom.org.uk/media-use-and-attitudes/attitudes-to-news/one-in-three-internet-users-fail-to-question-misinformation/.

[33] Verizon, “2024 Data Breach Investigations Report,” May 2024, https://www.verizon.com/business/resources/reports/dbir/.

[34] Lance Spitzner, “Why a Phishing Click Rate of 0% is Bad,” November 2017, https://www.sans.org/blog/why-a-phishing-click-rate-of-0-is-bad/.

[35] Shreya Ghosh, and Mitra Prasenjit, 2023. “Review of How Early Can We Detect? Detecting Misinformation on Social Media Using User Profiling and Network Characteristics,” in: Lecture Notes in Computer Science, edited by Gianmarco De Francisci Morales, Claudia Perlich, Natali Ruchansky, Nicolas Kourtellis, Elena Baralis, and Francesco Bonchi, Vol. 14174, Springer. https://doi.org/10.1007/978-3-031-43427-3_11.

[36] Idem.

[37] Frederico Monti, Fabrizio Frasca, Davide Eynard, Damon Mannion, and Michael M. Bronstein, “Review of Fake News Detection on Social Media Using Geometric Deep Learning,” in: Representation Learning on Graphs and Manifolds Workshop, ICLR 2019, May 2019, Ernest N. Morial Convention Center, New Orleans, USA, https://rlgm.github.io/papers/34.pdf.

[38] Microsoft, 2023, “Microsoft Digital Defense Report: Building and improving cyber resilience,” October 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

[39] Md Shohel Rana, Mohammad Nur Nobi, Beddhu Murali and Andrew H. Sung, "Deepfake Detection: A Systematic Literature Review," in: IEEE Access, vol. 10, 25494-25513, 2022, doi: 10.1109/ACCESS.2022.3154404.

[40] Yingtong Dou, Kai Shu, Congying Xia, Philip S. Yu, and Lichao Sun, 2021, July, User preference-aware fake news detection. In Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval (2051-2055).

[41] “DISARM Framework Explorer,” DISARM Frameworks, last modified November 2023, https://disarmframework.herokuapp.com/.

[42] EU Disinfo Lab, “Tools to monitor disinformation,” 2024, https://www.disinfo.eu/resources/tools-to-monitor-disinformation/.

[43] European External Action Service (EEAS), “2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A framework for networked defence,” January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf.

[44] EU Disinfo Lab, “Tools to monitor disinformation,” 2024, https://www.disinfo.eu/resources/tools-to-monitor-disinformation/.

The Janus-Faced Hybrid Nature Of Cyber-Related Technologies In The Cognitive Domain

JOSEF SCHRÖFL

SÖNKE MARAHRENS

Authors: Colonel Josef Schroefl started his career in the Austrian Armed Forces in 1982 and worked since then in various areas of the military, including several military operations/UN tours, e.g. to Syria. He holds a B.A. in Computer Technology and an M.A. in Intern. Relations from the University of Delaware/U.S. and a PhD in International Politics from the University of Vienna. Several publications/books on Asymmetric/Cyber/Hybrid threats, crisis, conflict and warfare. Current position: Deputy Director for CoI Strategy & Defense at the hybrid CoE in Helsinki/Finland, leading the Cyber-Workstrand.

Colonel Sönke Marahrens is a career Air Force officer, previously serving as head of research for Strategy and Armed Forces at the German Institute for Defence and Strategic Studies in Hamburg. As well as a Full Diploma in Computer Science, he holds a master's degree from the Royal Military College in Kingston, Canada, and another from the University of the Federal Armed Forces in Hamburg. He was deployed with NATO to Bosnia and Kosovo, and in 2020 served as Branch Head for Transition at HQ Resolute Support in Kabul, Afghanistan.
Current position: Head of the digital Development, German Armed Forces.

The views contained in this article are the authors' alone and do not represent the views of the Austrian MoD, the German MoD, or the Hybrid CoE.

Abstract: As a prerequisite to effectively identifying and countering cyber and hybrid threats, as well as cognitive warfare/superiority campaigns against Western democracies worldwide, it is crucial to have cross-governmental and international information-sharing capabilities. Due to the vast amount of data, this process must be supported by technically advanced AI/ML-powered technology to analyse multilingual and publicly available information in near real-time. Such monitoring systems must send timely alerts to specific decision-makers, supporting them in formulating appropriate responses to hybrid activities as part of emerging and evolving cognitive warfare campaigns from adversarial countries like Russia and/or the People's Republic of China.

Problem statement: How will cyber threats based on new / disrupting cyber-related technologies evolve?

So what?: Cyber-attacks exploiting vulnerabilities in artificial intelligence (AI) models are of particular concern in critical areas such as medicine, financial systems, and national defense, where AI-based decisions have important consequences. NATO and the EU must do everything to prepare our societies to promote a mindset that encourages questioning the integrity of information in principle, being more suspicious against signs of manipulation, minimising internal isolation, embracing the necessity of reporting suspicious behaviour, and fostering proactive calls for support within the wider community whenever necessary. Therefore, A stronger and more robust security culture is needed.

The Intersection of AI and Cybersecurity

The Russian attack on Ukraine is already in its third year. However, the war itself had been prepared long before in cyberspace and started well before any physical activity through cyber-attacks. Moreover, even the first physical strike in February 2022 was prepared in cyberspace: Within the first minutes of the military attack on Ukraine, Russia paralysed the KA-Sat satellite network. However, this attack had unintended consequences, disrupting many internet services in Europe.[1] In Germany, for example, 5,800 Enercon wind turbines were affected. In France, almost 9,000 subscribers to a satellite internet service also experienced outages. Other countries affected included Italy, Poland, Hungary and Greece.[2] Parallel to its activities in and around Ukraine, Russia has carried out an intensive campaign of hybrid warfare against Western societies to advance a couple of different strategic objectives, like isolating Ukraine, cracking Western support, and, unfortunately, being successful in gaining new allies in Africa and Asia. Russia's disinformation campaigns in Africa were successful in several countries, including Cameroon, Central African Republic (CAR), Côte d'Ivoire, the Democratic Republic of the Congo (DRC), Libya, Madagascar, Mozambique and Sudan. In Asia, Russia has influenced countries such as India, Indonesia, the Philippines, Malaysia, Japan, and South Korea. These campaigns often aim to promote pro-Russian narratives and undermine Western influence. The efforts typically focus on spreading

misinformation to influence public opinion and political processes.[3]

The means chosen included the destabilisation of Western democracies through the spread of conspiracy theories on the Internet and direct interference in Western elections,[4] attacks on ammunition depots in Bulgaria and the Czech Republic,[5] the murder of Russian regime opponents in Europe,[6] and massive cyber-attacks on critical infrastructure and public institutions. Russia has, for example, promoted numerous conspiracy theories around elections, particularly in the U.S. These include false claims about widespread voter fraud, the vulnerability of mail-in ballots, and the manipulation of voting machines.[6] However, also during the pandemic, Russia spread conspiracy theories about the origins of COVID-19, the safety and efficiency of vaccines, and the intentions behind public health measures. These theories aimed to sow distrust in governments and health authorities. Another common theme is the accusation that Western countries stage false flag operations to justify military interventions or political actions. These theories claim that events like terrorist attacks or chemical weapon use are orchestrated by Western governments to manipulate public opinion.[8]

Russia also often promotes conspiracy theories that paint Western countries, especially the U.S., as corrupt and manipulative. These narratives suggest that Western governments are involved in secret plots to control global politics and economics.[9] The conspiracy theories are disseminated through various channels, including state-controlled media, social media platforms, and sympathetic influencers. The goal is often to create confusion, undermine trust in institutions, and destabilise societies.

When the Russian attack began in February 2022, Western democracies were shocked. Although tough measures such as economic sanctions were threatened in advance, Russia was not deterred and attacked Ukraine on a broad front. In the beginning, Ukrainian and Russian diplomats also met to negotiate a ceasefire. After more than 2.5 years of war, however, a peace agreement seems a long way off. The West, still supporting Ukraine, and Russia have firmly positioned themselves as adversaries, a reality that will continue to persist, even if the guns in Ukraine fall silent. Cyberspace has blurred the lines between peace and war, making a new cold war undeniable.

In 2024, the cybersecurity landscape is more dynamic and challenging than ever. As cyber threats evolve, traditional defence approaches struggle to keep pace. AI-driven systems offer promising solutions. The need for reliable information and the sustainability of mainstream media that presents diverse political Perspectives is critically important in (2024) a year marked by pivotal elections in more than 40 democracies worldwide while wars continue to rage in Europe and the Middle East. Improving media literacy and fostering a more resilient society are key challenges. The same technology, which can be used to manipulate the infosphere, is also able to be leveraged for fact-checking, disinformation tracking, integrity and authenticity checking, credibility scoring, malicious spam/bot detection and blocking, and secure coding.

Hybrid Threats and AI - the Dark Twins

Hybrid threats combine conventional military tactics, cyberattacks, disinformation campaigns, and other non-traditional methods. These tactics blur the lines between state and non-state actors, internal and external, peace and war while trying to stay below the certain recognisable threshold, thus making attribution challenging:[10]

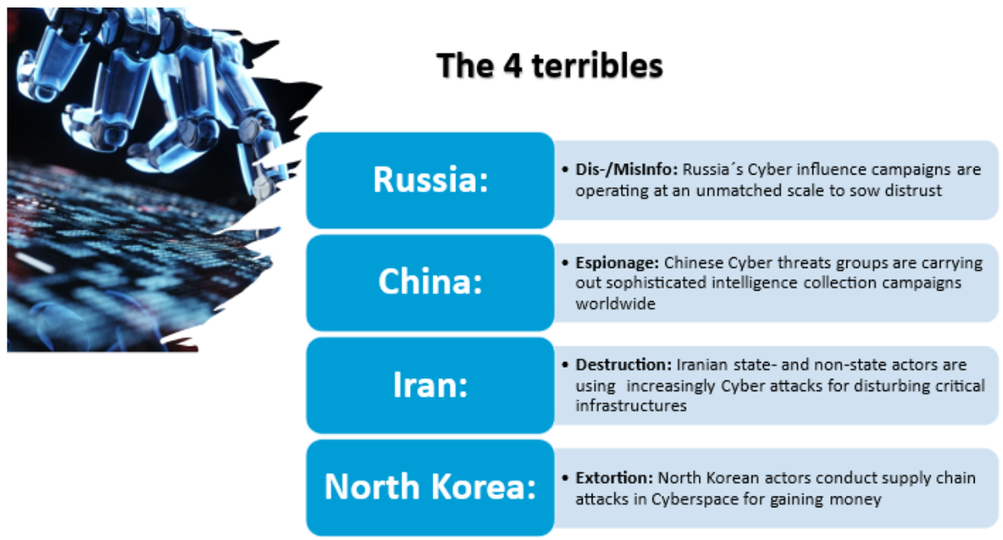
The use of AI amplifies hybrid threats

- More sophisticated cyberattacks: AI can automate and optimise existing processes and, therefore, also those which are used with a malign intent: cyberattacks become more and more potent. For example, AI-generated phishing emails can be better tailored to specific targets, increasing their persuasiveness and leading to more successful attacks. State or non-state actors might use AI to create false attribution trails and tracks, hiding the true source of an attack. AI can enable proxy attacks, where an actor uses AI tools to carry out an operation without direct personal involvement through (even artificial) proxies.[11]
- Disinformation campaigns: AI can create and amplify the dissemination of fake news, deepfakes, and manipulated content. As a consequence, trust in online information erodes and exacerbates hybrid threats many times over. AI-generated deepfake videos spread false narratives, manipulate public opinion, and undermine trust in existing information sources. AI algorithms amplify disinformation on social platforms, sowing discord and confusion.[12]
- The physical weaponisation of AI: AI can be used to automate cyberattacks, making them more efficient and widespread and can be used by terrorist groups or rogue actors to plan biological or chemical attacks. AI-driven malware enables rapidly propagating across networks, causing significant damage even on physical network elements. AI-powered drones or autonomous weapons carry out highly precise strikes, bypassing traditional defences and escalating conflicts.[13]

In conclusion, AI's impact on hybrid threats is multifaceted. It introduces new and more dangerous risks.

Hybrid threats in the cognitive domain

Cognitive superiority[14] can be seen as one of the decisive goals of modern information, cyber and hybrid warfare, relying on access to information, pervasive surveillance, personalised persuasion, and new technologies. While the concept of cognitive superiority is nothing new, its importance within the military domain- traditionally the primary carrier of defence -needs more systematic assessment, especially regarding its broader societal impact. Therefore, hybrid threats' broad field and impact must be viewed in a more differentiated and sophisticated way and manner.[15]



The cyber-specialties of the "4 terribles"; Source: Author.

Cognitive warfare-a relatively modern term in the field of hybrid threats-refers to a more holistic approach to cognitive superiority. Main goals of cognitive warfare are attacking societal leadership, influencing the perceptions of local communities as well as entire societies to disrupt or fragment societies and make them even more vulnerable or receptive to manipulation. Like other hybrid warfare tactics and techniques, cognitive warfare has, except for targeted killings, no kinetic component. Still, it could have direct physical consequences (e.g. through radicalisation) but usually stays below the threshold of open conflict(s).

Here, cyberspace has developed a Janus-faced nature. In addition to its advantages in fostering democracies through more transparency and participation, it has started also to facilitate the creation of a vitreous human and-potentially-transparent society.

The widespread use of digitalisation made the virtual cyberspace a place for “real meetings”, a diplomatic tool, an economic factor, a military effector, and last but not least: a social space, satisfying especially human needs for connectivity. On the one hand, cyberspace has democratised access to information as an unlimited, borderless and barrier-free space. On the other hand, however, it has "damaged" the Westphalian paradigm of the state as guardian of sovereignty almost to the point of its dissolution. By overriding the state’s monopoly of (physical) power, cyberspace has introduced new and different forms of power and even violence. Malign actors have direct access to influence almost every target audience, allowing them to set, undermine, or dominate intra-societal narratives.[16]

One of the biggest “hybrid” threats is malign actors’ activities to destabilise the foundations of the “Western” value-based cognitive domain by undermining core values, such as human dignity, freedom, democracy, equality, the rule of law and adherence to human rights are critical. Especially the “cognitive” battle for narratives in cyberspace, which is a reality. This battle seeks to dominate the cognitive domain and gain advantages by controlling the narratives. Currently, one of the most damaging impacts on society is the pervasive penetration of social media, which erodes empathy[17] and undermines existing elements of societal resilience from within.

The impact of new Technologies

One of the key issues of recent years that will keep the (Western) world busy for a long time to come is new technologies, in particular AI and Cloud computing. This development is being driven by the increase in existing data volumes and the use of this data. However, what often receives a lot of attention in exemplary projects does not necessarily correspond to reality.

Data has long been seen as the new gold: the Big Five of the technology industry, also known by the abbreviation FAANG (Facebook, Amazon, Apple, Netflix, Google), generated a market capitalisation of nearly 4 trillion dollars in 2023 to large extent from the use of information only.[18] Together with Microsoft’s 7 trillion dollar turnaround, the market capitalisation of information can be valued up to 11 trillion dollars, accounting for almost 25% of the U.S. stock market's total market capitalisation of $31 trillion.

New technologies are, therefore, obviously fundamentally changing the economy and society. They drive entrepreneurial innovation, productivity, and regional economic growth. They also affect growth, labour markets, and political participation. The consequence places new demands on education and training-not just in the area of information and communication technologies but also in literacy.

The ability to adapt to the changing world through the education and training system is of fundamental importance, especially from an educational societal perspective. In the future, the question of how fast and deep new technologies will penetrate (Western) societies and how they will change productivity, employment and competitiveness in different countries must be of central interest.

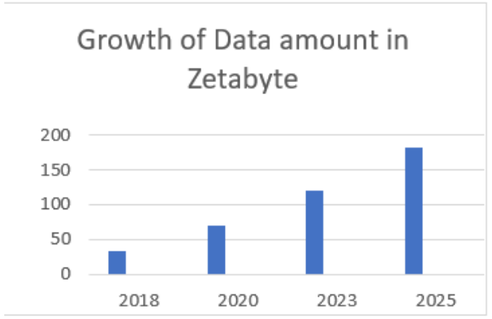
Example: The growth of data-amount[19]

1 Zettabyte (ZB) = 1 000 000 000 000 000 000 000 byte

1 zettabyte is equal to 1,000 exabytes or 1 billion terabytes.

Amount of digital data generated annually worldwide (in ZB, forecast for 2025):

- 2015: 15,5
- 2018: 33
- 2023: 121
- 2025: 181



Source: Author.

Technics needed, to deal with…

Quantum Computing

Quantum Computing expands the existing limits of conventional computing with their binary states of 1 or 0. Adding more states, the computing power increases significantly. Quantum researchers are implementing this idea using quantum physics to create and use quantum bits, also called “qubits”.

Qubits can represent superpositions of the states 0 and 1 as well as various intermediate levels. Thanks to these inherent properties, quantum computers are very powerful in theory. Currently, they still struggle with a high error rate. Once this problem is solved, quantum computers may even be able to crack cryptographic codes.[20]

Cloud and Edge Computing

Cloud computing forms the foundation for many future innovations in different technologies and applications:[21]

- Serverless IT architecture: In the future, companies and also governments will no longer need servers but will use a cloud infrastructure that they can scale at will.
- Artificial intelligence: AI requires huge amounts of data (big data), which are mostly available in unstructured form. In the future, these will be stored in the cloud and retrieved from there so that only the results need to be sent to the end devices.
- Smart city: In the city of the future, automobiles, buses and trains will drive autonomously, buildings will optimise their infrastructure independently and digitisation will make it easier to save energy. The corresponding data is stored in the cloud.
- Agriculture: Automation and precision farming promises more sustainable and, at the same time, more cost-efficient cultivation of the soil. To do this, the producers involved exchange information about cloud tools and share data on the germination rate.

Edge computing, as an extension of cloud computing, allows a shared approach between the cloud and the client. By mediating data processing between the device and the cloud, only the results of calculations have to be transmitted to the cloud. Thus, it reduces the latency of intelligent devices, leading to faster reaction times. Edge computing forms the basis for the Internet of Things (IoT) and Computing.[22]

Risk mitigation to maintain cognitive superiority (or mental health)

The war in Ukraine gives the impression of a return to the Cold War. A new political agenda has been created in North America and Europe that pits democracies against autocracies. However, the war in Ukraine has too many dimensions to be reduced to a simple conflict between democracy and autocracy. Such a simplification ignores the different levels and qualities of Western and European democracies. The lack of a democratic political system in Russia or China has not prevented North America or the European Union from entering into economic cooperation and increasing investment in and trade with these countries. A blatant example of this is the construction of the Nord Stream pipeline, which was supported primarily by Germany. Presenting support for Ukraine as a defence of democracy is a simplification designed to generate global support. In fact, it obscures the problem and conceals the fact that all European countries continued to do business with Russia even after Moscow annexed Crimea in 2014. It is, therefore, problematic to view the war in Ukraine from this binary political perspective of democracy and autocracy when it should actually be about the defence and inviolability of the borders between states.[23]

An inviolability that has never existed and will never exist in cyberspace. In cyberspace, since its inception, those who were ahead in the technology field have always had the advantage, but what is now even more important is the cognitive superiority that can be achieved in cyber and information space.

Both sides use targeted disinformation and propaganda to influence public opinion and weaken the enemy's morale. This includes the spread of fake news, the manipulation of social media, and the use of mass media to spread enemy images. Russia also uses historical narratives to underpin political goals. This instrumentalisation of history strengthens the identity and cohesion of its own population and underpins the legitimacy of its own position.

Under Vladimir Putin, for example, a historical narrative has developed in the Russian Federation that combines the ideology of the "Russian World". In short, an uncritical attitude towards the Russian Empire and a nostalgic glorification of the Soviet era, including the justification of Stalin's totalitarianism. The extreme cult of the "Great Patriotic War" is central to this narrative. It also served to convince the Russian population that the Soviet Union was a victim of the Second World War and that, for example, Finland was the first to attack it in the autumn of 1939, and that the Hitler-Stalin Pact is a myth of European historiography. In reality, World War II began exactly after the Hitler-Stalin Pact, in which both powers agreed to divide and occupy Poland, and it ended with participation in the war against Japan to conquer further territories. Reinforced by Putin's deception is, among other things, that the Russian population ultimately believes in Russia's invincibility.

Resume

In 2024, the cybersecurity landscape is more dynamic and challenging than ever. As cyber threats become more sophisticated and frequent, countries must prioritise robust security measures to protect their sensitive data and maintain operational integrity. Technological advances are changing the way nations approach cybersecurity, offering innovative tools and methods to stay one step ahead of malicious actors. It is critical for us to understand these changes to protect societies and ensure resilience in an increasingly connected world. The tools available for cybersecurity are evolving rapidly, from the integration of artificial intelligence (AI) and machine learning (ML) to the promising developments in quantum computing and blockchain technology. These advances are not only improving the ability to detect and respond to threats but are also introducing new paradigms and advanced cloud security solutions. These changes must be taken seriously and lead to proactively implementing advanced security measures that protect our democracies and keep us ahead in an increasingly digital world. The future of cybersecurity is here, and it is more powerful and dynamic than ever before.

It means that societal and political security are now two sides of the same coin. To destabilise democratic states, new technologies as a hybrid threat can be used in cyber operations, information warfare, cyber-enabled disinformation operations, foreign direct investment, as well as in social media to manipulate large numbers of people. Designing technology-driven, human-centred, community-driven accessible solutions for society as a whole is a significant step towards building deeper media literacy, fostering resilience and instilling a stronger security culture. These allow citizens to participate more easily in querying the integrity of information, identify signs of manipulation, minimise isolation, learn the importance of reporting suspicious behaviour, and ask for help within the wider community whenever necessary.

Endnotes

[1] Viasat is providing an overview and incident report on the cyber-attack against the KA-SAT network, which occurred on February 24, 2022, and resulted in a partial interruption of KA-SAT's consumer-oriented satellite broadband service. https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

[2] One of the cases described at the cyberconflict platform. https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

[3] An exemplary list of countries affected in Africa can be found on: https://africacenter.org/spotlight/russian-disinformation-campaigns-target-africa-interview-shelby-grossman/; the influence of Russia to African and Asian countries are described in the BBC report from February 2023: https://www.bbc.com/news/world-africa-64451376.

[4] John Irish, "European election: How the EU says Russia is spreading disinformation," June 03, 2024, https://www.reuters.com/world/europe/european-election-how-eu-says-russia-is-spreading-disinformation-2024-06-03/.

[5] The Bellingcat Investigation Team of volunteers and full-time investigators who make up the core of the Bellingcat's investigative efforts. https://www.bellingcat.com/news/uk-and-europe/2021/04/26/how-gru-sabotage-and-assassination-operations-in-czechia-and-bulgaria-sought-to-undermine-ukraine/.

[6] Steve Gutterman, "The List Is Long: Russians Who Have Died After Running Afoul Of The Kremlin," in: Radio Free Europe, February 16, 2024, https://www.rferl.org/a/enemies-kremlin-deaths-prigozhin-list/32562583.html.

[7] That example has also been described within the U.S. by the online-newspaper "Michiganadvance": https://michiganadvance.com/2024/10/25/firehose-of-election-conspiracy-theories-floods-final-days-of-the-campaign/

[8] Five Russian disinformation tactics have been excellently characterised in the online-journal "The Conversation": https://theconversation.com/five-disinformation-tactics-russia-is-using-to-try-to-influence-the-us-election-238379

[9] As described in the BBC-report: https://www.bbc.com/news/world-europe-64789737

[10] Common publication about Hybrid threats from Hybrid CoE, September 2023, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

[11] Thomas H. Davenport, Matthias Holweg, and Dan Jeavons, "How AI Is Helping Companies Redesign Processes," March 02, 2023, https://hbr.org/2023/03/how-ai-is-helping-companies-redesign-processes.

[12] Dennis Hillemann, "AI Misinformation Threatens 2024 US Elections," Medium, January 06, 2024, https://dhillemann.medium.com/ai-misinformation-threatens-2024-us-elections-72a3e804b383.

[13] Derived from a U.S.-Department of Homeland Security Report on Reducing the Risks at the Intersection of Artificial Intelligence and Chemical, Biological, Radiological, and Nuclear Threats from April 26, 2024, https://www.dhs.gov/sites/default/files/2024-06/24_0620_cwmd-dhs-cbrn-ai-eo-report-04262024-public-release.pdf.

[14] Even after three years of sharing one office, both authors still disagree on the notion of cognitive superiority: whereas Josef believes in it, Sönke still denies its existence - even vast amounts of Finnish coffee could not heal this.

[15] Outcome of the Cyber/Hybrid-Symposium took place on October 10, 2023 with the title "The relationship between hybrid warfare and cognitive threats studied from the cyber defence point of view," Hybrid CoE, https://www.hybridcoe.fi/news/the-relationship-between-hybrid-warfare-and-cognitive-threats-studied-from-the-cyber-defence-point-of-view/.

[16] Matthias Wasinger, "The Highest Form of Freedom and the West's Best Weapon to Counter Cogniti-

ve Warfare," May 20, 2024, The Defence Horizon Journal, https://tdhj.org/blog/post/freedom-counter-cognitive-warfare/.

[17] Bernard Claverie and François du Cluzel, "The Cognitive Warfare Concept," December 2023, https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf.

[18] The Corporate Finance Institute (CFI) is one of the leading global providers of training and productivity tools for finance and banking professionals. The Information is free and available on their homepage: https://corporatefinanceinstitute.com/resources/equities/faang-stocks/.

[19] Statista is a global data and business intelligence platform with an extensive collection of statistics, reports, and insights on over 80,000 topics from 22,500 sources in 170 industries. Established in Germany in 2007, Statista operates in 13 locations worldwide and employs around 1,100 professionals. The figures used are from the following source: https://www.statista.com/statistics/871513/worldwide-data-created/.

[20] This definition was taken verbatim from the article from Matt Swayne, "What is Quantum Computing? [Everything You Need to Know]," February 02, 2024, The Quantum Insider, https://thequantuminsider.com/2024/02/02/what-is-quantum-computing.

[21] Rafia Islam, Vardhan Patamsetti, Aparna Gadhi, Ragha Madhavi Gondu, Chinna Manikanta Bandaru, Sai Chaitanya Kesani, Olatunde Abiona, "The Future of Cloud Computing: Benefits and Challenges," in: International Journal of Communications, Network and System Sciences, Vol.16 No.4, April 2023, https://www.scirp.org/journal/paperinformation?paperid=124299.

[22] Idem.

[23] Ummu Salma Bava, "Democracies versus autocracies - this is not the new global conflict line," in: DER STANDARD Intl., June 18, 2023.

Aspects of Cognitive Warfare

Hybrid CoE

THE DEFENCE HORIZON JOURNAL

ISBN: 978-3-200-10166-1