POSITION PAPER ON COUNTERING HYBRID THREATS

Tweede Kamer der Staten-Generaal, Commissie Defensie, 18 December 2024

By Kenneth Lasoen

Dr Kenneth Lasoen is professor of Intelligence Studies at the University of Antwerp and senior fellow at the Knowledge Centre Security Intelligence (KSI www.kenniscentrumsecurityintelligence.nl). The contents of this paper represent the personal views and opinion of the author, and do not necessarily reflect those of any organisation with which he is affiliated.

Introduction: this is war

Hybrid warfare is simply war by another means, but war nonetheless.

Only to the utmost naïve or willfully neglectful is it still not clear that Europe's time of peace is severely threatened. A threat that will be fatal for Europe as it is today: the crucible of democracy, freedom and human rights. In fact, the war is already full on – except for the moment, it is only the Ukrainians who are doing the bleeding. *For the moment*.

The West may not want to acknowledge it as such, but it should be obvious by now that as far as its 'strategic opponents' are concerned, as authoritarian countries like Russia, China, Iran and others have been so diplomatically called, they see themselves as at war with the West. This war has been waged against democracies for years, except not kinetic until the aggression against Ukraine. After decades of disinformation, subverting democratic processes, and undermining social cohesion and the international rules-based order, the forces of authoritarianism, aligned in a new axis of evil, find themselves strengthened by the West's powerless and lackluster response to continuing aggression against Ukraine and elsewhere. Even when Ukraine's defeat would make a physical attack on another Western democracy and the NATO alliance much more likely – if only as a further test of the West's perceived weakness. Vladimir Putin and his like rolled those dice a long time ago. For too long they have been loaded in their favour.

An essential part of the strategy of the West's enemies has been the use of what we have come to describe as hybrid warfare, a series of covert actions and manipulations which fall outside the legal definition of war, but are potentially just as undermining and damaging for the victim as kinetic conflict, perhaps even more so. Hybrid warfare is a form of coercion that exploits the vulnerabilities of its target, be they legal, political, or economic restrictions and complexities, to subdue or weaken the target without resorting to the use of military force. Although equally aggressive and even destructive, hybrid operations are called 'legal grey zone'[1] operations because they remain below the thresholds of kinetic conflict, rendering the victim virtually powerless to respond in a way that deters the aggressor without seemingly overreacting. The exploited complexities and subterfuge employed in the execution of hybrid operations also makes timely detection extremely difficult, as well as adequately reacting to them. Hybrid warfare consists for

[1] D. Tromblay, *Political Influence Operations. How Foreign Actors Seek to Shape U.S. Policy Making* (New York: Rowman & Littlefield 2018), 205.

a large part of deception, or in military terms, psychological operations (PSYOPS) in all its facets (disinformation, undermining, sabotage).[2]

So far such operations have elicited not much more than a reactive response. Incidents are reacted to after they occur, and are wholly dependent on resilience to minimize their impact. Most counter hybrid strategy pivots almost entirely on resilience and reactive defence. For example, the first iteration of the European Union's approach to countering disinformation was only to debunk false information and implement sanctions against the perpetrators under the Cyber Diplomacy Toolbox. Nowadays, the Foreign Information Manipulation and Interference (FIMI) Toolbox is more advanced and includes some further steps, as does the Hybrid Toolbox, but the crux of the response remains reactive. The fact that in the meantime there are so many EU toolboxes in addition to national countermeasures arguably only adds to the complexity and further paralyses decision making processes towards an expedient response to the threat. But the essence seems to remain that, not unlike the sitting duck, the EU and its member states merely await the next attack to react and attempt to repair the damage.[3] This falls far short of a viable strategy to fight this phenomenon.

The maintenance of peace depends upon the accumulation of deterrents against an potential aggressor, coupled with a sincere effort to redress grievances. This position paper argues that past efforts to counter hybrid warfare fail and continue to fail because they are only reactive, and calls for adopting a more assertive strategy, based on offensive counterintelligence, with offence as defence for a motto.

Going against hybrid warfare: the need for a creative counterintelligence strategy

For the enemies of the West winning without fighting is at the centre of their national security doctrines. It is a strategy intended to subdue the opponent through psychological operations. The Russian doctrine is called 'reflexive control' and China refers to its 'Three Warfares' (political, psychological, legal).[4] These grey zone/subthreshold operations attempt to compensate the perceived asymmetry between their power and that of the West. Hybrid actors see this as entirely justified because they consider their actions self-defence against the West's perceived pursuit of interests that could be damaging to their own.[5] Authoritarian regimes feel themselves threatened by the West's adoption of essential freedoms, human rights, democratic rule of law and the international order. They therefore seek to subvert those values while at the same time eroding Western geopolitical power and advancing their own geopolitical preferences.[6]

[2] P. Cullen et al. *The Landscape of Hybrid Threats: A Conceptual Model* (Brussels: Publications Office of the European Union 2021); D. Betz, "The Idea of Hybridity" in: O. Fridman, V. Kabernik, & J. Pearce (eds.), *Hybrid Conflicts and Information Warfare. New Labels, Old Politics* (Boulder: Lynne Renner 2019), 9-24; R. Johnson, "Hybrid War and Its Countermeasures: A Critique of the Literature" *Small Wars & Insurgencies* 29 (2017), 141–163.
[3] K. Lasoen, *Realising the Hybrid Toolbox: Opportunities and Pitfalls* (Den Haag: Clingendael Institute 2022). European External Action Service, *2nd EEAS Report on Foreign Information Manipulation and Interference Threats* (Brussels 2024).
[4] M. de Goeij, "Reflexive Control: Influencing Strategic Behavior" *Parameters* 53 (2023), 97-108; A. Vasara, *Theory of Reflexive Control. Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy*, Finnish Defence Studies 22 (Helsinki 2020); S. Lee, "China's 'Three Warfares': Origins, Applications, and Organizations" *Journal of Strategic Studies* 37 (2014), 198-221.
[5] United States Senate Committee on Foreign Relations, *Putin's Assymetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security* (Washington D.C. 2018), 13-14; K. Pollpeter, "Chinese Writings on Cyberwarfare and Coercion" in: J. Lindsay, T. Ming Cheun & D. Reveron (eds.), *China and Cybersecurity. Espionage, Strategy, and Politics in the Digital Domain* (Oxford: Oxford University Press 2015), 155.
[6] J. Allen, F. Hodges & J. Lindley-French, *Future War and the Defence of Europe* (Oxford: Oxford University Press 2022), 97, 160-165.

The basic blueprint of a hybrid campaign is essentially that of a deception operation. Departing from a desired outcome or behaviour of the target, the process to achieve that is reverse engineered through determining what manipulations need to occur to make the target behave in the desired fashion and through what channels the appropriate stimuli need to be conveyed (or misled) and across what domains (political, military, economic, social, information).[7] The hybrid actor enjoys the advantage of operating in a grey zone and being able to cause effects in one of the domains through a completely different one, thus avoiding detection. The result is potentially severely destabilising for the target, whose sovereignty is diminished through limiting the action radius for policy making.[8]

The majority of such subthreshold activity is coordinated, executed or enabled by intelligence services, some of which are quite adept at what is sometimes referred to as 'the dark arts of intelligence'. Secrecy being their specialty, intelligence agencies are the best at maintaining deniability and obfuscation. Indeed, most hybrid and deception operations have (dis)information at their core, with a goal to disadvantage and demoralise adversaries.[9] Arguably the key to impeding hybrid operations might then be with the security function of intelligence services. Ensuring the protection and integrity of one's own information, while denying an adversary acquiring and misusing that information, falls under the discipline of counterintelligence (CI). In combination with counterespionage, CI can take on an offensive character not only defending against and analysing, but also degrading, penetrating, disrupting and manipulating an adversary's activities.[10] As Robert Wallace explains:

> *It will require an understanding of our adversaries' intelligence strategies and thus their larger designs against us. Such a strategy would allow us to anticipate their moves, neutralize their technical capabilities, and identify their spies. With this greater knowledge of the playing field, we would be able to develop options for optimizing the security of our own operations and for controlling the playing field through the use of disruption, deception, and disinformation. In this way, homeland defense becomes less a front line for engagement than a line of defense woven into the course of offensive operations – much as a "castling" move might be considered in a game of chess. And with this more intimate knowledge of the adversary, defensive counterintelligence would have greater options for response. In addition, should attacks occur, we could attribute them to the perpetrators and punish accordingly.*[11]

The key wording of the above is 'punish accordingly.' It means pushing back, the missing part of the current response against hybrid attacks. There is a need for a multidisciplinary counterintelligence strategy that does not only consist of awareness of what methods and instruments are employed to exploit vulnerabilities and detection thereof, since in that regard European security services already have a reasonably adequate information position, but also includes turning those methods and instruments against the hybrid actor.[12] The complexities of cross-domain deterrence are at play against an adversary employing the full spectrum of hybrid

[7] R. Clark & W. Mitchell, *Deception. Counterdeception and Counterintelligence* (Washington D.C.: SAGE 2019), 32-43.
[8] A. Mumford, *Hybrid CoE Strategic Analysis 24: Ambiguity in Hybrid Warfare* (Helsinki: Hybrid Centre of Excellence 2020); Tromblay, *Political Influence Operations*, xiv.
[9] J. Rovner, "The Elements of an Intelligence Contest" in: R. Chesney & M. Sweets (eds.), *Deter, Disrupt, or Deceive. Assessing Cyber Conflict as an Intelligence Contest* (Washington D.C.: Georgetown University Press 2023), 35: "There is something sinister about clandestine schemes because victims can't be sure that they have fully contained the damage, even after spotting the intrusion. Who takes the blame becomes a fraught question when there is no objective answer. Political controversy and bureaucratic infighting follow."
[10] J. Olson, *To Catch a Spy. The Art of Counterintelligence* (Washington D.C.: Georgetown University Press 2019), 40.
[11] R. Wallace, "A Time for Counterespionage" in: J. Sims & B. Gerber (eds.), *Vaults, Mirrors, and Masks. Rediscovering U.S. Counterintelligence* (Washington D.C.: Georgetown University Press 2008), 117-118.
[12] P. Davies, "Counterintelligence and First Lines of Defense in an Age of Hybrid Warfare" *Journal of Intelligence, Conflict and Warfare* 6 (2023), online.

tools and for whom few rules apply.[13] Only counteroffensive measures can enable retaking the initiative.

Conclusion: the time to act is now

Owing to past neglect, in the face of the plainest warnings, we have now entered upon a period of danger greater than has befallen civilization since the last war.

The astute reader might recognise in some of the previous sentences an echo from the speeches of the now seemingly extinct breed of actual European statesman. For Winston Churchill's words about what threatened civilization in 1938 were as prophetic then as they are now. Perhaps he would have said today as well that Europe's leaders "go on in strange paradox, decided only to be undecided, resolved to be irresolute, adamant for drift, solid for fluidity, all-powerful to be impotent." He could warn once more that failure to act now may be seen in Europe as only giving away the interests of Ukraine, whereas such a course would deeply compromise, perhaps fatally endanger, the safety and independence of the EU and all its member states. That procrastination, half-measures, soothing expedients and delays will soon present their consequences. That there cannot be peace with powers "who spurn ethics, cheer their onward course by barbarism, vaunt the spirit of aggression and conquest, derive strength from persecution, and use, as we can see, with pitiless brutality the threat of murderous force."[14]

Hybrid campaigns are a threat only because we permit them to be so. They operate in the grey zone of international politics, a zone wherein the West constantly cedes terrain rather than defends it. While diplomacy and sanctions have been tried without much success so far, most of the EU's member states have simply taken hybrid attacks in their stride, reacting to them but remaining at a loss for how to deter and prevent. This has only encouraged the adversaries, as recent escalations in sabotage of critical infrastructure and direct interference with democratic processes, such as the 2024 Romanian presidential elections, to keep pushing the boundaries. Defending those boundaries and the grey zone between peaceful coexistence and armed conflict is up to the West. The time has come to signal more compellingly what the boundaries are and that they will be enforced.

Though certainly not the panacea of countering hybrid threats –it would be too limiting to reduce this fight to a counterintelligence question alone–, rethinking the role of counterintelligence practices might be a good starting point for devising a strategy that shows some teeth. Counterintelligence and counterdeception principles are key to understand, but can also penetrate, and thwart opponents. The latter needs to happen more to achieve cross-domain deterrence: to signal the willingness and capability to fight back. Turning hybrid operations against the culprits and creating a hostile operating environment to make our societies less fertile ground for subversive activities could even the playing field a little, ensuring freedom from attack by having freedom to counterattack. And it does not even require starting from scratch to do so. The principles of counterdeception have been studied and their methodologies provide a good basis for what needs to be undertaken now. There are options available for democratic countries with accountable security services. In the past these tactics have been utilised by Western countries, but they do need modernising and an ethical and legal framework.[15] In international politics as in sports, the best defence is offence.

[13] J. Lindsay & E. Gartzke, "Cross-Domain Deterrence, from Practice to Theory" in: J. Lindsay & E. Gartzke (eds.), *Cross-Domain Deterrence. Strategy in an era of Complexity* (Oxford: Oxford University Press 2019), 4.
[14] Quotes are from Churchill's speeches in the House of Commons, as edited by D. Cannadine, *Blood, Toil, Tears and Sweat: The Great Speeches* (London: Penguin 2002).
[15] See Tromblay, *Political Influence Operations,* 217-221. L. Johnson, "On Drawing a Bright Line for Covert Operations" *American Journal of International Law* 86 (1992), 284-309. One of the more comprehensive contributions to counterdeception literature is M. Bennett & E. Waltz, *Counter-Deception Principles and Applications for National Security* (Artech House: Norwood 2007).

Easier said than done however. Adopting a policy of greater assertiveness and denying adversaries the initiative through offence as defence poses a great deal of politically sensitive and ethical challenges, and the risk of escalation rather than de-escalation. Although in that regard it could be argued the situation is one of lose-lose: either we keep tolerating the attacks and suffer increasing infringements, or we strike back and risk escalation that way. The existing approach however must be revisited to address the severe mismatch between the possibilities of our adversaries to undermine our sovereignty and our possibilities to stop them from doing so. Mark Galeotti rightly argues that "the good guys, if they get their acts together, can use the same instruments as effectively as the baddies."[16]

To once again reiterate Churchill: we can no longer blind ourselves to the great change which has taken place in the geopolitical and military situation and to the dangers we have to meet. We must recognise that the forces of authoritarianism are at war with democracy and liberty, and that Europe must prepare immediately to defend its values with the collective strength of the world's most powerful economic bloc. The EU should add a sharp end to its foreign policy: "rearmament exceeding the war machines of the axis powers and accumulating enough deterrents to credibly send the signal that the West will defeat any campaign against the security of its civilisation and freedom."

Universiteit Antwerpen
Sint-Jacobstraat 2, 2000 Antwerpen
kenneth.lasoen@uantwerpen.be

Kenniscentrum Security Intelligence
Rijnzathe 8, 3454 PV Utrecht
klasoen@kenniscentrumsecurityintelligence.nl

[16] M. Galeotti, *The Weaponisation of Everything. A Field Guide tot he New Way of War* (New Haven: Yale University Press 2022), 6.