No. 155
February 2022

SECURITY POLICY BRIEF

Hybrid Warfare Is Not Synonymous with Cyber: The Threat of Influence Operations

Bernard Siman

The recent cyber-attack on Ukraine's governmental websites, widely attributed to Russia, has reinforced the widely held perception equating Hybrid Warfare with hostile cyber activities. This overlooks the broader and devastating impact that hostile influence operations can have on the economic and defence spheres. These operations are strategically more insidious and destructive. Unlike cyber operations, influence operations can run over a long period of time. Whereas the EU is reasonably well-equipped to deal with hostile cyber operations, awareness of and countermeasures against influence operations are surprisingly weak both at member state as well as at EU level.

Cyber operations form a key tool in the spectrum of the Hybrid Warfare "Toolbox". Hybrid Warfare is indeed not a way of war, but it is rather a collection of tools dynamically combined and deployed in different configurations as policy objectives alter. But Cyber is only one tool. The toolbox is rich with a variety of instruments. When a particular combination of tools is deployed it may change over time, as the desired ends dictate. These "ends and means" are continually re-assessed to ensure, to the extent possible, that attacks remain below the threshold of war. Such assessments is where the risk of miscalculation resides, leading potentially to armed conflict if the threshold is crossed.

These "means leading to ends" are deployed by the "Attacker" to weaken and soften up the Target, and deployed by the "Target" to protect or deter against the Attacker's hostile Hybrid operations. These operations generally deliver maximum effect for powers that are militarily inferior compared to other powers in order to compensate for this weakness by essentially undermining the speed, efficiency of, and trust with which political decisions are made. That includes those political decisions, requiring public support, to activate a military response and deploy in reaction to hostile action by an adversary state. Weakening political support for defence spending is another target of such influence operations. Both Russia and China have weaker military capabilities than NATO and have consequently developed an advanced Hybrid Toolbox with which the EU has to deal in an effective and timely manner to protect its interests.

Cyber operations attract attention and capture the imagination of the public and the institutions of the state because they are tangible, measurable, fathomable, with immediate and sometimes visible effects, and in some cases with consequences in the physical world. Hybrid Warfare has existed since the dawn of conflict,

though protagonists lacked the massive force multiplier created by cyber capabilities which turbo-charge the impact of Hybrid operations. This is evident in the speed of distribution of disinformation, for example, such as through social media, creating "parallel truths" that weaken socio-political cohesion. Moreover, it can lead to the loss of control over vital functions and data (e.g. infrastructure, banking, health, etc.). For the political masters and for corporates in democracies, cyber is a relatively easier domain to defend, as it is a well-defined "hard" area of security and defence, to which budgets, expertise, and practices can be devoted. They can also demonstrate to their constituencies that they "did something about it". The "Soft" hostile Hybrid tools of "Influence", however, is much harder to fathom, and to react to, by politicians, the media, and state institutions.

Influence Operations and Defence

Hybrid Warfare, therefore, covers the much broader range of Influence operations. These seek to undermine trust in the target's system, through mis/dis information, coercion, corruption, "Lawfare", Threat Finance, "DeepFakes", assassinations and "Active Measures", use of "useful idiots", and criminal activities. Trust is the corner stone of the democratic system, enabling it to reach decisions through its processes and institutions. Therefore, such attacks can have strategically devastating consequences by undermining trust in the system, by sowing division in societies along its myriad fault lines of language, ethnicity, religion, economic status, and so on. The creation of new perceptions to rival established truths is a key objective of Attacker states. This tool uses a grain of truth as anchor for a disinformation campaign in order to create a veneer of credibility for a totally false narrative, disseminated rapidly and massively through cyber.

This applies directly to defence. As mentioned earlier, a key aim is to weaken the support of the public for military responses and deployments. For example, "Lawfare" has been deployed to smear our armed forces by using existing laws to bring "vexatious" court cases against soldiers, falsely accusing them of human rights abuses. Deepfakes can also be used to falsely depict abuses by NATO soldiers on deployment.
The result is two direct effects that are crucial to the Attackers' overall strategic objectives at a time when their military capabilities are inferior to NATO's:

(1) Delay political decision making on military response and deployment, as the public trust in its armed forces weakens and politicians dither, affording the attackers time and space to consolidate (also politically) their gains on the ground.

(2) Delay military procurement and any modernisation drive as politicians follow public opinion that has already been successfully manipulated.

Influence Operations and the Economy

There is a further crucially important area that is threatened by the slow but strategic creep of "Influence Operations", and that has increasingly acquired a direct bearing on defence and security: economic and corporate activity and technology innovation. The control of Patents (IPs) for dual use technologies should be a key defence concern. Whoever masters the mysteries of new game-changing technologies quicker will also have game-changing strategic advantages (e.g. Quantum Computing and Artificial Intelligence). But this is not just about the future. At present a key realistic and possible threat to the economic, military, technology, and corporate combine concerns acquiring controlling shareholdings in EU companies developing and operating cutting-edge dual use satellite technology that can offer the best support available to hypersonic missiles. Such hybrid influence operations should be an urgent EU priority.

The political, military, security, intelligence as well as corporate leaders must up their game by confronting the uncomfortable fact that Influence operations may not even primarily target the defence companies per se, thus being much less visible as hostile actions. Rather they also target private sector companies that have nothing in principle to do with the military, such as

advanced manufacturing, software development and service companies, digital platforms, and crucially the space industry.

The commercial Space sector should become a key area requiring specific attention in terms of countering Influence Operations. In terms of the hardware elements of the space industry, the cost of launching vehicles into space is falling enabling states to leverage the commercial space activities for military ends. A key area of military use is the technologies that are of particular interest to adversaries, such as the development and deployment of hypersonic vehicles to carry military assets and deploy them quickly. The more sensitive area is the "software" elements, in particular the commercialisation of data in space. Data and its control are the key new geopolitical and military battleground akin to the dawn of the nuclear weapons age in the mid-1940s. In pure military terms the operations of the armed forces' digital backbones, stretching from the satellite to the platoon commanders, guiding missiles and supporting both decision making as well as operations, may well start to determine the military balance among the world's great powers in the four domains of land, sea, air and information. As military capabilities are broadened by these private-sector-led developments, the race is on as to who will acquire a particular IP first. This is the principal area in which hostile influence operations must be countered although seemingly unconnected directly to the military. This is particularly the case because our military innovation, development and procurement model relies on the private sector. China and Russia, however, rely on private-state partnerships and cooperation in which national objectives (e.g. AI, 5G and Quantum Computing) guide research and development. Our need, therefore, to protect our strategic IPs within the private sector must become an urgent priority.

In a legal sense, our private sector companies are the owners of these strategic Patents. The question of "who" controls the shareholding, the boards, and the management of these companies must become a key national security concern. This is so because owners and managers of companies control whether the recipients of their new technological findings are friends or foes. Hybrid operations against such companies (to acquire their IPs) are not the stuff of thrilling stories for the media, the public, political establishment, and state institutions. They are, moreover, not always acquisition operations led by a clearly identifiable "foreign investor" that can be subjected to scrutiny and screening under the "Foreign Direct Investment" category. Moreover, such acquisitions can be completed by EU-based and licenced companies with funds already in the EU's banking system, but whose ultimate beneficiaries may be Russian or Chinese, or others for that matter. Until 2018 some of the Baltic states still had a de facto "off-shore" banking system whose clients were mainly Russian. These funds are presumably still circulating in the EU and can easily be used to acquire companies deemed strategically useful to adversaries.

Other scenarios may see opportunistic or targeted exploitation and misuse of Environmental, Social and Governance (ESG) issues in publicly listed companies to force a change of shareholding, board, and management. DeepFakes may also be used in such influence operations to falsely depict politicians, corporate executives or auditors, for example, making statements indicating a much weaker financial position of their companies, or of the standards to which they adhere. The speed with which social media can distribute these DeepFakes before the truth is re-asserted (if at all successfully), could lead to a collapse in share prices, run on a bank (if it is falsely claimed that it is insolvent), and ultimately even civil unrest. It could lead to delaying the deployment of critical technologies and infrastructure affecting economic development and growth, e.g. 5G, nuclear energy and waste treatment, and vaccines.

A further direct security and defence threat through such hostile economic influence operations is "Technology Leak" from EU companies acquired by adversary state-sponsored companies, possibly to their proxy non-state actors. Belgium is particularly vulnerable: in 2018 it ranked eighth globally in the number of patents per million inhabitants, ahead of Japan. Many EEA states also made the first seven. COVID has caused significant cash flow problems in many companies offering opportunities for hostile influence operations

to acquire shareholdings in small and medium sized technology companies. Defence, security, technology, and the economy are totally interconnected in Hybrid warfare Influence Operations, and urgent action is crucial.

CONCLUSION

We urgently need to build resilience, as well as the high-quality response required to deal with influence-induced crises, not just in the Cyber domain, but crucially in the economic domain as well. Public-private partnership is key to building resilience and crisis management capabilities. A cornerstone of this partnership is to build a trusted network within which information can be exchanged in a secure environment. An Economic Security and Intelligence capability, operating this partnership and assembling the "collage" of disparate information and data into a coherent picture of the threat posed by Influence Operations, can become the institutional framework for such an effort.

A bureaucratic and business culture shift is required to make state institutions take an interest in economic influence operations in the same way they take other (more visible) threats seriously; whilst business needs to acknowledge and comprehend that not all market activity is benign, and to trust the state with what they are facing. The timing for such a shift in culture and institutional frameworks is opportune as citizens, business, and the state share the common interest of defending our prosperity, security, and way of life. All three are materially and directly threatened by Influence Operations much more than by cyber per se. Business as usual will have dire consequences for our societies. The only way to defeat hostile Influence Operations is by developing and adopting a new modus operandi that relies on collaboration of the different state institutions on the one hand, and between the state and the private sector on the other. The ministries of economy, finance, and infrastructure must become an integral part of the national security equation. The longer-term threat in the Ukraine beyond cyber-attacks lies in exactly this insidious mixture of strategic influence operations. The EU must assume that similar threats to its own economic, technology, and military combine are already present, and it must act urgently and decisively.

Bernard Siman is a Senior Associate Fellow at Egmont, and the Head of Financial Diplomacy at the Brussels Diplomatic Academy of the Vrije Universiteit Brussel. He also teaches at its Faculty of Social and Economic Sciences and at the Belgian Royal Military Academy. He was the UK Special Representative to the UAE for Financial and Professional Services. He advises governments and corporates on geopolitics and hybrid warfare, as well as on the Mediterranean region and Japan.

EGMONT Royal Institute for International Relations