The new war is everywhere

Over the past handful of years, new terms have appeared to describe the sense of a constant state of conflict across the world: hybrid warfare, cyber war, grey-zone conflict, misinformation, disinformation, malinformation, influence operations and malicious actors. They are just a few of the new phrases that have worked their way into the lexicon of conflict conversation in an attempt to define the new, relatively nebulous conceptions of confrontation between states that has begun to be the norm in times of peace. Most fall within the idea of «hybrid warfare».

Peace, as we know it, may be described as an absence of war. At the same time, war, in our traditional conception, is a conflict that becomes kinetic in nature, involving weapon strikes, troop commitments and armed conflict; but hybrid war has been changing our idea of peace time. According to NATO, hybrid war obscures «the line
between war and peacetime» while increasing ambiguity and vagueness on where possible hybrid attacks originate from by fusing unconventional as well as conventional tools of power, blurring the threshold of war (see Bargués & Bourekba, this volume).

Though not defined in such terms, the idea of hybrid war is as old as the well-worn pages of Sunzi, who wrote that the skills of warfighting could be encompassed in the idea of subduing «the enemy without fighting» (see Arco Escriche, this volume). Though this passage tends to be interpreted as suggesting that politics and other means should avert war, the idea of continuing or beginning a conflict outside of a kinetic battle has persisted throughout time.

In The Road to Unfreedom, Timothy Snyder (2018) noted that a risk with categorising hybrid warfare is that, due to its unconventional and non-kinetic nature, the confrontation can be perceived as «war minus» or less than a normal war. Snyder argues that this should really be seen as a «war plus» as it creates an environment of ongoing fight even without a kinetic element (Snyder, 2018: 157).

All these different notions of hybrid warfare give strong places to start on defining a purposely vague concept. In simple terms, hybrid warfare could be considered as the aggression from one entity (be it a state or faction) toward another with the use of non-kinetic tools of power with the intention of creating a strategic outcome. However, more work is needed to comprehend what hybrid war is in its current state. In particular, it should be important to delve into the factors defining when a state can consider itself in a hybrid war, what form the response should take, and if there are certain parameters that escalate conventional statecraft or power exertion between states into a hybrid war.

**Disinformation as a threat**

Hybrid warfare is like an octopus where every tentacle is a new, unconventional warfare tactic. But this octopus’ strongest tentacle is harnessing information as a weapon. As hybrid warfare has become more common, there has been a marked increase in the spread of what is categorised as misinformation, disinformation and malinformation (MDM). According to the United States Cybersecurity & Infrastructure Security Agency (CISA), the differences between these terms are slight but important to understand. Disinformation is information created deliberately to «harm, or manipulate a person, social group, organization, or country», while misinformation is false information created without intent to harm. Finally, malinformation is using
truthful information out of context in order to mislead. But the star of these tactics is disinformation.

Disinformation has been a growing threat in the past decade, as social media platforms continue to expand largely unchecked and dominate the news. But as disinformation grows, so do our strategies to quantify and battle it, and there are steps that can be taken to mitigate its effects.

Traditionally, we have identified and measured disinformation by focusing on the «production» side of disinformation; or on how much content has been created, «published, shared, or viewed»; or on metrics such as how many bots can be identified on Twitter. While these measures are effective for identifying sources of disinformation, they do not measure the impact of the information being pushed. While both metrics are important to measure, it is crucial to understand the efficacy of these campaigns.

On the production side of disinformation, the European Union approved in April 2022 a new legislative package to strengthen EU’s response to disinformation: the Digital Markets Act (DMA) and the Digital Services Act (DSA), that includes an updated Code of Practice on Disinformation which aims to tackle the spread of disinformation across technology platforms by making the platform owner (such as Meta, Twitter, etc.) liable for not curbing the spread of disinformation at its root. The Code approaches this by increasing reporting requirements by «very large online platforms» on their work countering disinformation, promoting fact-checking, increasing transparency in political advertising, and more. The penalties for not abiding by these rules may lead to fines of up to 6% of yearly global revenues.

Beyond this effort to create a regulatory framework that places certain limits on the phenomenon, new analytical measures are also advancing to increase knowledge about how disinformation spreads, as well as its social and political effects. One effective proposal for analysing the impact of a disinformation campaign is to measure whether, in the long run, this misleading content eventually leads to action, or if the content breakouts from the platform where it originates to be disseminated through other
channels. Ben Nimmo, in a report for Brookings, has worked to create a «breakout scale», which measures the impact of a piece of disinformation. This scale ranges from one to six, measuring if the disinformation leaves a single platform, if it jumps between different media sources, if it becomes amplified by celebrities and, finally, if it calls for action, violence, or policy measures. Working in concert with metrics to measure the root source of disinformation, this scale can help researchers understand the what, where, who and how by which disinformation takes root and spreads. But, all of these measures are for naught if they do not rebuild confidence in our democracies. The problem with disinformation is its potential for the erosion of democracies, but there are ways to combat this.

**How does democracy survive in a world of hybrid threats?**

Hybrid warfare and disinformation weaken the bases on which our democracies stand and violate the principles and rights upon which they were founded. That is the point of these tactics. But the threats have become so complicated that a fundamental question arises: Does democracy need to be rethought as a concept? Simply put: no, it doesn't. However, democracy, institutions and regulations do need to be revised to be still relevant in the digital era. Just as religious texts are interpreted for modern days, democracies must be interpreted and grown if they are to remain powerful enough entities to protect those inside of them. When it comes to regulating the tech industry to protect from disinformation campaigns, there are multiple steps that can easily be taken to create change right now.

Until 2014, Mark Zuckerberg’s mantra for Facebook was the well-known «move fast and break things». This saying meant to give Facebook’s developers and managers free reign to try, build and fail, and it was appropriated across Silicon Valley. Many tech companies like Uber and WeWork attempted to replace things like taxis and offices, and the results were mixed at best. What moving quickly and breaking things often lacked was oversight or thought about how new solutions could be misused.

Even if Zuckerberg’s mantra might have worked as a mindset for the tech industry, it could not be more antithetical to the slow, methodical and deliberative ideals of democracy. Democracies were designed from the outset to incorporate checks and balances meant to moderate their actions in order to make well-informed decisions to serve the people. This process was not meant to be fast or destructive. Faced with competition from an industry which can build totally new technologies in days, democracy finds itself unevenly matched.
Democracies are as relevant today as they were when the first democracy was born in Athens thousands of years ago. But many are still working under the strict precepts of their founding documents, having not thought to update themselves for a totally different world. In the United States, for example, the country was founded with what was seen as a «Living Constitution», meaning that it should be updated as the world changes – other states have also included this idea in their founding documents. But practice has proven to be a different matter in both the United States and other countries. As Walter Lippman wrote in 1919, democracies are influenced by the information available to them and must work to «control their environment» – this includes new information environments.

However, democratic regimes tend to be reactive instead of proactive, and it has taken nearly three decades to see strong regulations created to rein in this new tech world. Generally, democracies step in when a new sphere of influence becomes dangerous. In the United States, when the automotive industry began to grow unchecked, the National Highway Safety and Traffic Administration was created in 1970; and when pollution began to spread unrestricted across the country with the creation of the Environmental Protection Agency, also in 1970. When we look at the spread of disinformation, it is clear that the tech industry has become dangerous, and it is high time to take measures to make sense of the situation.

Nowadays, given the disruptive capacity of disinformation, amplified by the technology industry, the time has come to take measures to counter risks. Today, Mark Zuckerberg, the original advocate of moving fast and breaking things (who has since updated his motto to “move fast with stable infrastructure”), says that the government needs a more active role in regulating the internet and has put forth four simple regulations that could make social media and the internet a safer place: a) regulating harmful content, b) ensuring election integrity, c) privacy controls and d) data portability. Adopting these concepts would create a safer online environment.

The European Union is blazing a path ahead on creating a safer environment online with the above mentioned Digital Markets Act and Digital Services Act. The adoption of the DMA and DSA frameworks by major allies of the European Union would ensure consistent global regulation that helps prevent online pockets where bad actors can operate. Finally, 61 nations have signed the Declaration for the Future of the Internet proposed by the Biden administration, which sets out a global vision for the internet in which human rights are protected, competition is moderated, infrastructure is secured, and universal access is granted, among other topics. This document could be a strong first step towards achieving these goals if the signatories
would ensure that they abide by these rules, and if this document were created as an agreed-upon legal framework instead of its current state as a nonbinding agreement.

As discussed, there are numerous ways democratic institutions can survive and grow in the current environment. First, stronger definitions of hybrid warfare and parameters on what constitutes being in a hybrid conflict would cut through the vagueness that these tactics seek to create. Next, using data to measure the effectiveness of acts within conflicts, such as the spread of disinformation, can help gauge risk and reaction. Finally, implementing updated rules and regulations can help safeguard the public and give institutions the latitude they need to work in a new world of threats. Democracies were created to grow and adapt, and it is high time they do.

References


