

Addressing asymmetric and hybrid threats against the Philippines

Sherwin Ona

The evolving nature of warfare underscores the need to recognize its complexity and its peculiarities. The ongoing conflicts in Europe and the Middle East illustrate the rapid evolution of modern warfare, becoming more asymmetric and frequently incorporating hybrid strategies. Additionally, while its main objective is to disrupt an opponent's decision-making capacity and reduce their ability to resist, both state and non-state actors, together with their proxies, continue to be the key players in this emerging battlespace.

Often conducted below the threshold of armed conflict, asymmetric warfare is characterized by ambiguity, intimidation, and coercion among others. Gray-zone tactics fall within this domain. In addition, the weaponization of cyberspace and the manipulation of information are the defining characteristic of this approach. While its hybrid counterpart complements these efforts by integrating diplomacy, politics, economics, and military power to achieve strategic objectives.

A defining feature of this new conflict environment is the growing use of disinformation techniques and the convergence of espionage activities with malign influence and offensive cyber operations. Digital technologies remain to be at the center of this insidious effort. For instance, artificial intelligence (AI) and social engineering techniques are used to exploit the open and interconnected nature of the Internet. While AI-enabled cyber-attacks and quantum computing capabilities are projected to upend traditional cybersecurity practices, thereby undermining national security, individual privacy rights, and intellectual property regimes.

In Europe, the Russian invasion of Ukraine seemingly integrated traditional military techniques (i.e. Kinetic actions) with asymmetric approaches. For instance, both sides displayed a penchant for psychological and information operations using social media. This is combined with the innovative use of drones in their kinetic operations. However, a more ominous aspect of this conflict is the alleged plan to weaken NATO's resolve. The rapid spread of false narratives in the region, the drone incursions in Germany and Poland's irregular immigration challenges, seem to point to the persistent use of asymmetric techniques.

A similar playbook can be seen in Taiwan, where its democratically elected government has been subjected to continuous threat from China. While a full-blown invasion remains a possibility, the Taiwanese society is constantly subjected to asymmetric-hybrid aggression such as disinformation campaigns, malign influence operations, and economic coercion

among others. In addition, Taiwan is known to experience 20-50 million cyber-attacks per day, allegedly targeting critical infrastructure, government systems, and its citizens.

The Philippines is not exempt from this phenomenon. China's belligerent actions in the West Philippine Sea are often viewed as the most visible manifestation of this strategy. However, focusing merely on the maritime aspect risks overlooking the less visible dimensions of asymmetric-hybrid warfare. For instance, the latest allegations raised against Philippine Vice President Sara Duterte concerning bank deposits reportedly made by Chinese state-owned enterprises amounting to PhP 500 million, seem to show signs of foreign interference. In addition, the controversies surrounding former mayor Alice Guo and the candidacy of former governor Joseph Cua raised questions about their citizenship and their alleged links to China's intelligence network. It has also intensified concerns about possible elite capture. Similarly, statements by several Filipino senators that appear to echo narratives undermining the Philippine position in the West Philippine Sea, seem to support this observation. These incidents illustrate how domestic politics may be manipulated by a foreign malign actor to foment confusion and aggravate political divisions, resulting in the possible weakening of national resolve. In addition, these incidents are compounded by disinformation campaigns that seek to shift blame for maritime tensions onto the Philippines, portray the country as lacking strategic autonomy, and advance frivolous Chinese sovereignty claims over Philippine territories, including Batanes and Palawan provinces.

Overall, asymmetric warriors love to exploit vulnerabilities. They know that democratic institutions are usually siloed and are bound by good governance principles. Malign actors see this as a "weak system" that can be abused. Moreover, malign actors see victory beyond the traditional battlefield. They strongly believe that the new battlespace exists in cyberspace and the cognitive domain.

At this juncture, it is crucial for Filipino leaders and policy makers to "connect the dots" and avoid fragmentation and dissipation of effort. Democratic societies might be vulnerable to some extent, but I strongly believe that it is with these same governance principles that we can get ahead of these threats.

We are not alone in this fight. Best practices from Europe and Asia can provide valuable insights in developing a national resilience strategy. At the policy level, Finland's Comprehensive Security Model and Singapore's Total Defense Concept offer excellent frameworks on how to adopt an integrated, whole-of-society approach. A key feature of this level is enacting legislation on the protection of critical infrastructure and improving existing cyber-crime laws, as well as penalizing the spread of disinformation. A strategic communication program is also a vital component of this level.

At the operational and organizational level, opening spaces for participation for non-government stakeholders remains one of the vital pillars of resilience. In open market

societies, much of the critical infrastructure is in the hands of the private sector. Their combined talents and resources create a pool of expertise that government alone cannot match. While at the individual level, the ability of civil society organizations and the academe to develop education and research programs is a vital component of national resilience.

Another crucial element of this effort is leadership. Armed with strategic foresight and collective action techniques, countering asymmetric-hybrid threats depends on the country's leaders to present a strategic and coherent vision of an end state. Moreover, moving from a deterrent posture to societal resilience requires government leadership and the cooperation of various sectors. Leadership entails the capacity to create participation spaces, define the roles of various stakeholders, and identify the desired outcomes as well as the allocation of resources.

In closing, countering asymmetric-hybrid threats requires a *all-hands-on-deck*" approach. We must all recognize its complexity as part of the evolving nature of conflict. Specifically, we need to understand that this concept draws from the confluence of goals and non-traditional strategies as well as the use of unconventional tools that allow its malign use below the threshold of a kinetic war.

Therefore, the Philippines must quickly learn from the experiences of other countries. The country must acknowledge its weaknesses and vulnerabilities while pursuing ways on how to address them. With national resilience as its end goal, it must strengthen its democratic institutions to avoid institutional and elite capture as well as pursue a robust deterrence posture.

About the Author



Dr. Sherwin E. Ona is an associate professor of political science and development studies at De La Salle University. He is a senior fellow of the Philippine Public Safety College and the Stratbase Institute. Dr. Ona is also an alumnus of the DKI-Asia Pacific Center for Security Studies and an international fellow of the Institute for National Defense and Security Research of Taiwan. He is an officer of the Philippine Coast Guard Auxiliary with the rank of commander.