

RSIS Commentary is a platform to provide timely and, where appropriate, policy-relevant commentary and analysis of topical and contemporary issues. The authors' views are their own and do not represent the official position of the S. Rajaratnam School of International Studies, NTU. These commentaries may be reproduced with prior permission from RSIS and due recognition to the author(s) and RSIS. Please email to Mr Yang Razali Kassim, Editor RSIS Commentary at RSISPublications@ntu.edu.sg.

Future Warfare: The Two-Dimensional Security Challenge

By Steven Metz

SYNOPSIS

While it is difficult to precisely predict the future of armed conflict, two things seem likely: Asia will be the vortex of the global security system; and armed conflict will have both conventional and hybrid dimensions.

COMMENTARY

IT IS impossible to predict the evolutionary path of armed conflict, in part because human decisions can send history spinning in unexpected directions. Imagine, for instance, what today's global security system might look like had not a small group of Al Qaeda leaders distracted the United States from the high tech "revolution in military affairs" that it was pursuing before the September 11, 2001 terrorist attacks.

The future of armed conflict will, like its past, be determined by the interplay of broad trends and human choices. But despite the difficulty of precise prediction two things do seem clear: Asia will form the vortex of the global security system; and armed conflict will have both conventional and hybrid dimensions.

The Two Dimensions of Armed Conflict

The conventional dimension of armed conflict will be shaped by the growing assertiveness and expanding military power of China. There may be conventional war between other nations but any conflict involving China will, by definition, be strategically significant.

Technology will be central in the conventional dimension of armed conflict, especially artificial intelligence and robotics. The speed and complexity of military engagements will exceed the decision-making capability of humans, thus warfighters will

increasingly rely on artificial intelligence. This will generate both technological challenges -the adversary with the most effective artificial intelligence system will have an advantage - and ethical ones.

Algorithms and data sets will become centres of gravity to be attacked and defended; strategic and operational concepts will need to account for this. Because much of the technology required for conventional warfighting will be adapted from the interconnected global private sector, technology will disperse rapidly.

No nation will be able to assume that it will have or can preserve aggregate technological superiority. Advantages will be situational and transitory. promoted is that of a low tax (even tax haven), unregulated, small government laissez faire paradise.

Weaponisation of Everything

In open political systems there may be public opposition to things like soldier enhancement technology (to include human-technology cyborgs) and killer robots. Authoritarian regimes will be able to quell or ignore any public opposition to these sorts of technologies. This could give them a leg up during conflicts with nations where the public does have a say.

While large scale conventional war will be the most dangerous, conflicts in the hybrid dimension will be the most common. Polyglot, often shifting coalitions of states, proto-state organisations, transnational organised crime, and mercenaries will use armed action to advance their interests, deter adversaries, and attain psychological effects.

This will be war deep in the shadows: nations which become involved may do so clandestinely to avoid the political pressure or sanction that overt involvement might bring, relying on proxies instead of direct involvement.

Hybrid conflicts will often involve foreign fighters, sometimes significant numbers of them, and will have transnational, even global implications. People far from the actual fighting will play a role by narrative shaping, attention swarming, and the provision of information and other resources.

Hybrid conflict will be characterised by the "weaponisation of everything" rather than reliance on weapon systems developed explicitly for warfighting. Think of the use of airliners for the September 11 attacks on the United States, the use of recreational drones for military surveillance, social media attacks on foreign political systems, and cyberattacks on infrastructure.

In the broad sense the ongoing conflicts in Syria and Ukraine are emblematic of what the hybrid dimension may look like. Both have dragged on for years with no end in sight, and both have cascading destabilising effects both in their region and globally. Both are characterised by intricate complexity centered on psychological effects.

What This Means

Nations cannot ignore either dimension of the security environment. If they focus exclusively on one, their adversaries will exploit the other. But the capabilities and skills needed are different in the two dimensions.

In the conventional dimension speed and the ability to function in the face of intricate complexity will determine success. Speed will mean both speed of action and speed of decision in an avalanche of information, much of it deliberately false or misleading. The most successful militaries will be those which at least exploit - and if possible master - the convergence of humans and technology.

Avoiding or minimising deception will be crucial, requiring a blend of technology and human judgment. Military operations will involve swarming and dispersing across domains rather than traditional phasing.

In the hybrid dimension adaptability and the ability to create tightly integrated, holistic security organisations and concepts will be the keys to success. Adaptability will be in play not only at the operational level, but strategically and organizationally - nations must be able to design and refine new security organisations as challenges evolve.

Security Leaders as Cutting Edge Entrepreneurs?

Security leaders and strategists must, in other words, be cutting edge entrepreneurs akin to those in the most dynamic realms of the private sector. And because psychological effects matter more than kinetic ones in the hybrid dimensions, dynamic narrative shaping will be decisive. Strategists must be psychologically astute, effective communicators rather than simply the manager of battles.

Today every nation must build methods to develop the skill sets needed for the two dimensions of conflict, not only in their militaries and other government agencies, but across their societies and within the community of their security partners.

They need communities of practice and simulation based on the needed skills, refine psychological and educational tools to identify and develop the skills, and organise their security organisations to recruit, retain, award, and empower people with the skills needed in both dimensions of conflict.

No nation can know in advance which dimension will be most important to it at any given time, but all will need effectiveness in both. As the nature of security and conflict change, so too must the organisations and concepts to address them.

Steven Metz is Senior Research Professor at the US Army War College Strategic Studies Institute and a non-resident fellow at the Quincy Institute for Responsible Statecraft. The ideas in this commentary are strictly those of the author and do not represent the official position of the US Army or US Army War College.
