ASAN
PLENUM
2015

TALKING POINTS

Asan Plenum 2015: "Is the U.S. Back?"
www.asanplenum.org

RELEASE EMBARGO DATE: April 28, 2015 at 9:00 AM

Panel: Cyberwar
Date/Time: Tuesday, April 28, 2015 / 15:30-16:45
Talking Points for: Michael Raska, S. Rajaratnam School of International Studies

Over the last two decades, political leaders, military officers, and civilian strategists have struggled to understand the impact of cyberspace on conflict and war. The U.S. military has termed cyberspace as a separate military domain in line with traditional war fighting concepts tied to the air, land, sea, and even nuclear domains. However, cyberspace as a separate domain has been too narrow a term for understanding the global complexity of information and cyber conflicts that transcend boundaries of land, sea, air, institutions, and nations. Indeed, the importance of cyber is not its conceptualization as a separate domain, but what significance it has for strategic outcomes.

Seen from this perspective, the question is where, how, and why may cyber conflicts actually shape the future of East Asian strategic landscape? In particular, how will the use of "cyberspace" help select states in East Asia achieve their political or strategic objectives? What can we say about cyber warfare and cyber espionage as tools to solve regional political disputes? Do cyber conflicts increase the likelihood of major escalation in East Asian 'hot spots' such as the Korean Peninsula? How will cyber capabilities, defensive or offensive, augment traditional military capabilities of major powers in the region, and more importantly, help their strategies achieve desired political outcomes? Ultimately, will cyber conflicts represent a major threat to strategic instability between major powers in the region, particularly the United States and China?

These questions highlight the strategic significance of the on-going information revolution and progressive complexity of cyber threats, which are increasingly blurring distinctions between civil and military domains, state and non-state actors, principal targets and weapons used. As more governments, intelligence agencies, military organizations as well as non-state actors invest in developing cyber capabilities, future conflicts—particularly in East Asia—will be increasingly linked with confrontations in and out of cyber space, cyber-attacks on physical systems and processes controlling critical information infrastructure, information operations, and various forms of cyber espionage.

Indeed, the continuously evolving multi-dimensional character of information and cyber operations enables new types of "force multipliers"—the ability to operate rapidly against distant adversaries without the commitment of combat personnel; the ability to act in secret by minimizing exposure, attribution, and subsequent risks of counterattacks; the ability to use cyber weapons as disrupt, deny, destroy, or subvert key nodes of critical national

* The views expressed herein do not necessarily reflect the views of the Asan Institute for Policy Studies.

infrastructures, including communications systems, banking and finance, logistics and transportation systems, national databases, and other vital information grids.

Arguably, we are entering the next wave of “hybrid” computer network operations that combine select elements of cyber and information warfare, which are gradually translated into the “kinetic” or “physical domain.” The conceptual development of hybrid wars is evident in the Russian, Chinese, and, to a lesser degree, North Korean strategic thought on future conflicts. Underscoring Russia’s concepts of “hybrid wars”, for example, are three mutually-reinforcing principles. First and foremost is the idea of the “permanency of conflict,” which blurs the boundaries between wartime and peacetime, space and time, as well as actors involved. In essence, ascertaining whether a state of war exists becomes increasingly difficult, particularly for the one under an attack.

The second characteristic of emerging hybrid conflicts is “multidimensionality.” Specifically, achieving political and strategic objectives are no longer bound solely to traditional conventional military means; what is more important is the confluence of political, economic, informational, and other non-military means that, in turn, achieve the desired strategic effects, while also reducing the necessity for deploying hard military power to the bare minimum. Hybrid warfare, therefore, compels the opponent’s military and civil population to support the attacker, to the detriment of their own government and country.

The third defining principle is “unified effort”—simultaneous application of “mixed tactics” conducted across the enemy’s entire territory, and more importantly, within its “spheres of influence.” In Russian, Chinese, and North Korean strategic thought, the main battlespace is inside the mind of the enemy. Therefore, hybrid warfare is as much about the primacy of “influence operations,” including elaborate internal communications, deception operations, psychological operations, and well-defined external strategic communications in the cyber domain. These “invisible operations” subsequently pave the way for the “kinetic” victory on the battlefield.

The diffusion and adaptation of hybrid concepts that link cyber-kinetic-information strategies will likely shape the future of East Asia’s strategic landscape. This is because hybrid warfare is generally about situations where conflict may be ambiguous, such as in the context of the Korean Peninsula and territorial disputes in the East and South China Seas. Armed fighting may not yet have occurred, but the war is already raging psychologically, politically, economically, and in the cyber arena. On one hand, its manifestation in cyberspace may be so subtle and incremental, and the information war so abstruse, that a state may not recognize its long-term strategic impact. On the other hand, hybrid “cyber-kinetic” strategies are becoming a part of new power-projection capabilities in select militaries in East Asia—complementing existing aerospace and naval assets, standoff precision weapons, ballistic and cruise missiles, and space-based C4ISR systems.

Hybrid warfare is therefore shaping the development of new domains of “military rivalry” in

* The views expressed herein do not necessarily reflect the views of the Asan Institute for Policy Studies.

East Asia—outer space, underwater, cyber & near space. Taken together, it challenges South Korea's traditional national defence strategies and conceptions. South Korea has to search for new strategic thought that would translate select elements of hybrid warfare to its own advantage.

Michael Raska is a Research Fellow at the Institute of Defence and Strategic Studies, a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.

* The views expressed herein do not necessarily reflect the views of the Asan Institute for Policy Studies.