Written Representation 97

Name: Michael Raska
Assistant Professor

Received: 1 Mar 2018

Cyber-Enabled Information Conflicts in East Asia: Implications for Singapore

Michael Raska, Ph.D.
Assistant Professor

S. Rajaratnam School of International Studies
Nanyang Technological University

Key Findings:

When contemplating how future information and cyber conflicts may affect Singaporean security and defense requirements, the Singapore Government should consider the following:

- Singapore needs to explore the nature of the evolving strategic competition in East Asia, which includes cyber-enabled information conflicts. In this context, Singapore may become vulnerable to political and "hybrid" warfare. This is because as conflicts evolve parallel in the cyber and information domains, the centers of gravity are also going to shift. The value and more importantly, the accuracy and reliability of strategic information relevant for the situational awareness and function of the nation state as a system will become even more important with the increased dependence on cyberspace.

- As more governments, intelligence agencies, military organisations as well as non-state actors invest in developing cyber / information warfare 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. The resulting "cyber-kinetic conflicts" will evolve parallel with technological changes – e.g. the introduction of next generation of robots, artificial intelligence, and remotely controlled systems that will continue to alter the character of future warfare.

- The character of hybrid conflicts in the regional "gray zones" may also likely reflect low-level intensity conflicts in "peripheral information/influence campaigns", rather than high-end conflicts – given the considerable escalatory risks. Cyber-enabled information operations – defensive, offensive, and intelligence-driven increasingly serve as a key enabler and force-multiplier of kinetic operations – enabling actions, capabilities, and effects of land, sea, air, and space operations in all physical domains. Under the changing character of conflict, Singapore and the SAF will likely have to redefine its objectives necessary to achieve "victory."

- These issues highlight the strategic significance of the progressive complexity of cyber-enabled information threats, which are increasingly blurring distinctions between civil and military domains, state and non-state actors, principal targets and weapons used. In this context, cyber-enabled information operations enable and reinforce strategic ambiguity in terms of effects, sources, and motives, and therefore can be used to deny or create political outcomes without visible military commitments.

- Notwithstanding the variance in different strategic cultures and doctrinal conceptions on the use of cyber/information means as instruments of warfare, the use of online activities and behaviour for political aims will have increasingly offline consequences, and vice-versa.

Cyber-Enabled Information Conflicts

Notwithstanding the conceptual, organizational, and technological integration of cyber operations (COs) - whether defensive, offensive, or intelligence-driven into military affairs over the last two decades, “considerable uncertainty surrounds the strategic impact of cyber instruments of warfare,” including information operations.[1] These merge “cyber-technical” and “cognitive-psychological” attacks, which are waged during peacetime and wartime, simultaneously in domestic and external information spheres. Unlike the use of conventional weapons – i.e. for defense, deterrence, coercion, or swaggering - the use of cyber-enabled information weapons – embedded not only in malicious codes and hardware, but also in the use of information as an instrument of national power – is predicated on the ability to access and exploit adversary’s networks, physical infrastructures as well as media undetected. The unpredictability of consequences or potential cascading effects of cyber and information operations further strengthens the incentives for secrecy, opacity, and ambiguity in cyberspace. Direct, and to a lesser degree, indirect results of cyber/information attacks are often invisible, which raises uncertainties on the sources of the intrusion or system malfunction. Even if the source is known or detected, the purpose of cyber-attacks might be less clear.[2] The more opacity a state reveals about its cyber capabilities and their intended use, the more an adversary can predict potential attack vectors and prepare to mitigate targeted vulnerabilities.[3]

At the same time, the progressive complexity of cyber and information operations is reflected in cross-domain strategic interactions – between cyber, physical, and cognitive information domains, civil and military spheres, state and non-state actors.[4] This interconnected environment amplifies the strategic importance of cyberspace, which is increasingly used for political, economic, military, technological, media, and ideological

[1] Thomas, Mahnken, ‘Cyber War and Cyber Warfare’, in Kristin Lord and Travis Sharp (eds), *America's Cyber Future: Security and Prosperity in the Information Age* (Washington DC.: Center for a New American Security, 2011), p. 53-62.

[2] Martin Libicki, 'The Strategic Uses of Ambiguity in Cyberspace', *Military and Strategic Affairs*, vol. 3, no.3, 2011, p.3-10.

[3] Greg Rattray and Jason Healey, 'Categorizing and Understanding Offensive Cyber Capabilities and Their Use', In National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington DC: The National Academies Press, 2010), p.77-98.

[4] US Joint Staff, Joint Force Development, Cross-Domain Synergy in Joint Operations: A Planner's Guide (Washington D.C.: US Department of Defense, 2016), http://www.dtic.mil/doctrine/concepts/joint_concepts/cross_domain_planning_guide.pdf

struggles for influence that challenge traditional security conceptions.[5] Social media, for example, provide new tools for both state and non-state actors to seed ideas, deliver tailored information campaigns, and in doing so, influence events or environment in real time. In other words, the use of social media campaigns in conflicts is becoming as important as winning the military campaign.[6] The resulting complexity of interactions create systemic effects that have significant consequences on how states achieve their core national security objectives.[7]

With the increasing sophistication and diffusion of cyber-enabled information threats, state actors are searching for new strategies to leverage cyber/information capabilities into effective instruments of warfare. In the US strategic context, for example, the latest cyber strategy aims on five key objectives: (1) building and maintaining ready forces and capabilities to conduct cyberspace operations; (2) defending military information networks, securing data, and mitigating risks; (3) preparing to defend the US from disruptive or destructive cyberattacks of significant consequence; (4) developing viable cyber options and plans to control conflict escalation and shape the conflict environment at all stages; and ultimately, (5) build and maintain robust international alliances and partnerships to deter shared threats.[8] Cyber and information operations, however, are constantly evolving, principally as a result of continuous adaptation to developments in cyberspace such as proliferation of malicious code (malware), diffusion of advanced military technologies, and operational experiences and lessons-learned. Conceptualizing and assessing advanced cyber and information conflict trajectories is therefore a challenging task.

Despite these caveats, there are a number of applicable frameworks that view the development of information warfare in the context of “cyber power” – the relative means, resources, methods, and capacities used to convey power in or through cyberspace.[9] In

[5] Michael Raska, ‘Cyber Conflicts and Singapore’s ‘Total Defence’ Strategy’, *RSIS Commentary*, 23 June 2016, https://www.rsis.edu.sg/rsis-publication/rsis/co16156-cyber-conflicts-and-singapores-total-defence-strategy/#.WEZUOfl96Hs.

[6] Leong Tai Liang, 'Battlefront New Media – Lessons for The SAF Based On a Study of the Information Campaign During Operation Pillar of Defence', *Pointer - Journal of Singapore Armed Forces*, vol.41, no4, 2015, p.55-68, https://www.mindef.gov.sg/safti/pointer/documents/pdf/V41N4_battelfrontnewmedia.pdf.

[7] Spencer Bakich, 'Conceptualizing Emerging Strategic Challenges in the Cyber Age', *The Bridge*, 13 December, 2016, http://thestrategybridge.org/the-bridge/2016/12/13/conceptualizing-emerging-strategic-challenges-in-the-cyber-age.

[8] US Department of Defense, 'The DoD Cyber Strategy', 2015, p.13-15, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[9] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power* (London: International Institute for Strategic Studies, 2011), http://www.iiss.org/en/publications/adelphi/by%20year/2011-2c64/cyberspace-and-the-state--toward-a-strategy-for-cyber-power-4bb1.

particular, cyber power capabilities will reflect a number of dimensions in both civil and military domains such as (1) national cyber security policy and strategy, (2) cyber culture and society, (3) cyber security education, training, and skills, (4) legal and regulatory frameworks, and (5) standards, organizations, and technologies.[10] At the same time, cyber power will also depend on the presence of military-organizational structure (if any) related to cyberspace and the state's known views on the use of cyberspace by its armed forces.[11] The resulting "cyber maturity" matrix provides a scale of approximate capability development – from the lowest levels implying a non-existent or limited level of capacity to the highest level, characterized by a dynamic approach, effective implementation, and operation of cyber-defense related structures, policies, legislation and organizations.[12]

At the operational level, one can also try to ascertain the level of sophistication in cyber and information operations based on *capability requirements and available resources*.[13] However, the line between low-end and high-end cyberspace and information operations is frequently blended – a sophisticated state actor can employ non-state actors as proxies, apply low-cost, off-the-shelf tools available on the free market, and exploit known vulnerabilities and techniques such as denial of Service (DoS) attacks, or use artificial intelligence and botnets. At the same time, however, a sophisticated state actor can engage in resource-and intelligence-intensive operations that *discover* vulnerabilities in systems (Zero-Day exploits) as well as in political/strategic cultures apply strategies of denial, disruption, destruction, or subversion of information or physical infrastructure. Such operations, whether strategic or tactical in nature, can also range in duration from short to long-term, and typically follow a series of steps: (1) reconnaissance, (2) weaponization, (3) delivery, (4) exploitation, (5) installation, (6) command and control and, (7) actions on objectives.[14]

At the high-end of cyber-enabled information conflicts are "existential cyber-attacks" characterized as "causing sufficient wide scale damage for the government potentially to lose control of the country, including loss or damage to significant portions of military and

[10] The Global Cyber Security Capacity Centre, 'Cyber Security Capability Maturity Model (CMM) – V1.2', 15 December 2014, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf.

[11] ASPI International Cyber Policy Centre, *Cyber Maturity in the Asia Pacific Region* (Sydney: Australian Strategic Policy Institute, 2016), https://www.aspi.org.au/publications/cyber-maturity-2016/ASPI-Cyber-Maturity-2016.pdf.

[12] The Global Cyber Security Capacity Centre, 'Cyber Security Capability Maturity Model (CMM) – V1.2', 15 December 2014, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf.

[13] Joseph Nye, Cyber Power (Boston: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2010), p.11, http://belfercenter.hks.harvard.edu/files/cyber-power.pdf

[14] Eric Hutchins, Michael Cloppert, and Amin Rohan, 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains', In: Leigh Armistead (ed.) *Proceedings of the 6th International Conference on I-Warfare and Security* (Washington D.C.: The George Washington University, 2011).

critical infrastructure: power generation, communications, fuel and transportation, emergency services, financial services, etc."[15] Such attacks would be complemented with the use of disinformation, concealment, and deception campaigns to create an atmosphere of pressure that would aim for the target population or state into a decision objectively leading to its own defeat. In other words, generate maximum uncertainty within a target society, and in doing so, reduce the necessity for deploying military hard-power for political purposes to the minimum.

Figure 1. Cyber Defense Capability Matrix

Categories	Start-Up	Formative	Established	Strategic	Dynamic
Strategy	National security policy and defense strategy may be published and may contain a digital or information security component.	Specific threats to national security in cyberspace have been identified, such as external threat actors (both state and non-state), insider threats, supply systems vulnerabilities, and threats to military operational capacity, but a coherent response strategy does not yet exist.	National cyber defense policy/White Paper exists and outlines the military's position in its response to different types and levels of cyber-attacks (for example, cyber enabled conflict producing a conventional, kinetic effect and offensive cyber-attacks aimed to disrupt infrastructure including emergency response).	National cyber defense complies with relevant international law and is consistent with national and international rules of engagement in cyberspace. Resources dedicated toward engaging in international cyber defense forums are allocated based on national strategic objectives.	The evolving threat landscape in cyber security is captured through repeated review in order to ensure that cyber defense ways and means continue to meet national security objectives. Rules of engagement are clearly defined and the military doctrine that applies to cyberspace is fully developed and takes note of significant shifts in the

[15] Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, (Washington DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2013), p. 2, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

					cyber security environment
Organization	Informal management of cyber defense may be distributed among the armed forces and/or government organizations, with occasional reference to signals intelligence. There is no clear command structure for cyber security in the defense apparatus.	Cyber operations units are incorporated into the different branches of the armed forces, but no central command and control structure exists.	There is a defined organization within the Defense ministry responsible for conflict using cyber means	Highly specialized expertise with advanced strategic cyber capabilities and full situational awareness are integrated into the national defense strategic posture.	Defense ministry contributes to the debate in developing a common international understanding of the point at which a cyber-attack might trigger a cross-domain response.
Coordination	The national defense apparatus contains no (or limited) capacity for cyber resilience (intended to reduce vulnerabilities to national security interests).	Cyber defense capability requirements are agreed between the public and private sector in order to minimize the threat to national security incurred by both sectors.	The need for coordination in the event of exfiltration of digital information by malicious actors is recognized and prepared for. Defense organizations and critical infrastructure providers have established a mechanism to report	Some analytical capacity exists to support the coordination of and resource allocation for national cyber defense; possibly including a cyberdefence research center.	The entity in charge of cyber defense coordinates strategic integration regarding cyber events between government, military and critical infrastructure including budgets and identifies clear roles and responsibilities. This process then feeds into the re-

			threat intelligence.		evaluation of the national security posture of the nation.

Source: "Cyber Security Capability Maturity Model" (CSMM), The Global Cyber Security Capacity Centre, University of Oxford (2014), https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf.

Figure 2. Cyber Threat Taxonomy

Tier	Description
I	Practitioners who rely on others to develop the malicious code, delivery mechanisms, and execution strategy (use known exploits).
II	Practitioners with a greater depth of experience, with the ability to develop their own tools (from publically known vulnerabilities).
III	Practitioners who focus on the discovery and use of unknown malicious code, are adept at installing user and kernel mode root kits, frequently use data mining tools, target corporate executives and key users (government and industry) for the purpose of stealing personal and corporate data with the expressed purpose of selling the information to other criminal elements.
IV	Criminal or state actors who are organized, highly technical, proficient, well-funded professionals working in teams to discover new vulnerabilities and develop exploits.
V	State actors who create vulnerabilities through an active program to "influence" commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest.
VI	States with the ability to successfully execute full spectrum (cyber capabilities in combination with all of their military and intelligence capabilities) operations to achieve a specific outcome in political, military, economic, etc. domains and apply at scale.

Source: Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, (Washington DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2013.

Evolving Doctrinal Variations

In Asia-Pacific, the paths and patterns of military cyber diffusion – the process of international transmission, communication, and integration of cyber-related military concepts, organizations, and technologies - reflect varying trajectories and capabilities across different strategic cultures. To begin with, the US military has traditionally distinguished between (1) defensive; (2) offensive; and (3) intelligence operations – employed in varying levels during peacetime, crises, and wartime.[16] At the same time, the US has applied a compartmentalized approach to kinetic and cognitive or psychological spheres of cyberspace operations and information operations (IOs). The US military doctrine regarding cyberspace, *Cyberspace Operations* (JP 3-12R 2013), for example, views cyberspace operations as "the use of cyberspace capabilities to create effects which support operations across the physical domain and cyberspace,"[17] while IOs are concerned with the "integrated employment of information-related capabilities during military operations…to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own."[18] In practice, however, the dividing lines between cyber "intelligence", "offensive" and "defensive" missions are intertwined. The changing strategic thinking can be seen in the latest 2015 US *DoD Cyber Strategy* calls for "integrated, adaptive, and dynamic defensive operations."[19]

China's military conceptions on cyber and information operations have been also changing.[20] In 2016, the PLA has embarked on a series of major reforms in its organizational force structure, following the release of updated military strategic guidelines (2015) that call for the PLA to fight and win "Informationized Local Wars."[21] The 2016 military reforms created a new command structure – the Joint Staff Department under the Central Military Commission (CMC), inaugurated three new services (PLA Ground Forces, PLA Rocket Forces and PLA Strategic Support Forces), and reorganized major PLA military commands from the previous seven "military regions" to five "major

[16] For example, in the U.S. DoD terminology, defensive cyberspace operations (DCO) refer to internal defensive measures, response actions, and countermeasures, whether passive or active "to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems." Offensive cyberspace operation (OCO) capabilities include actions "to degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time." Or they can be used "to control or change the adversary's information, information systems, and/or networks in a manner that supports the commander's objectives." (OCO) are "intended to project power by the application of force in and through cyberspace." Cyber Intelligence Operations (CIO), include intelligence, surveillance, and reconnaissance (ISR) activities in cyberspace "conducted to gather intelligence that may be required to support future operations, including OCO or DCO. These activities synchronize and integrate the planning and operation of cyberspace systems, in director support of current and future operations."

[17] US Department of Defense, 'Joint Publication 3-12(R) Cyberspace Operations', 2013, p.5, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

[18] US Department of Defense, 'Joint Publication 3-12(R) Cyberspace Operations', 2013, p.5, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

[19] US Department of Defense, 'The DoD Cyber Strategy', 2015, p.20, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[20] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington D.C.: Department of Defense, 2013),p.10, http://archive.defense.gov/pubs/2013_China_Report_FINAL.pdf

[21] Information Office of the State Council of the People's Republic of China, *China's National Defense in 2015*, 26 May 2015, http://eng.mod.gov.cn/Database/WhitePapers/index.htm.

war zones" (Northern, Eastern, Southern, Western, and Central).[22] In this context, PLA's cyber operations - technical reconnaissance, electronic warfare, network reconnaissance, defense, and attack operations, previously conducted by the General Staff Headquarters Third and Fourth Departments, have been elevated into the PLA's Strategic Support Forces (SSF).[23] With revised military strategic guidelines, revamped organizational force structure, and operational concepts, the PLA has expanded the scope of its "core missions" that now include "protecting national security interests in space and cyberspace."[24]

For the PLA, achieving "information dominance" (*zhi xinxi quan*), controlling electromagnetic spectrum, while prioritizing computer network defense represent key prerequisites for air and naval superiority as well as for establishing "space dominance" (*zhi tian quan*).[25] In this context, the PLA is conceptualizing "integrated strategic deterrence" through a holistic representation that includes simultaneous and coordinated use of offensive and defensive electronic warfare (EW), military space and counter-space, along with "network reconnaissance" and "network attack and defense operations" in varying security conditions - peacetime, crisis, and war.[26] According to the 2015 Defense White Paper, "the development of the world revolution in military affairs is deepening" while "the form of war is accelerating its transformation to informationization."[27] Its strategic assessments of the "form of war" have changed from "integrated operations, precision strikes to subdue the enemy," articulated in the 2004 *Defense White Paper*, to "information dominance, precision strikes on strategic points, joint operations to gain victory." [28] In this context, the PLA has prioritized the development of long-range, precision, smart and unmanned weapons and equipment, and space and cyber operations.

[22] Phillip Saunders and Joel Wuthnow, 'China's Goldwater-Nichols? Assessing PLA Organizational Reforms', Joint Forces Quarterly, vol.82, no.3, 2016, p.68-75, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-82/jfq-82_68-75_Saunders-Wuthnow.pdf.

[23] John Costello, 'The Strategic Support Force: China's Information Warfare Service', The China Brief, vol.16, no.3, 2016, https://jamestown.org/program/the-strategic-support-force-chinas-information-warfare-service/.

[24] Michael Chase, Jeffrey Engstrom, Tai Ming Cheung, Kristen Gunness, Scott Warren Harold, Susan Puska and Samuel Berkowitz, *China's Incomplete Military Transformation: Assessing the Weaknesses of the People's Liberation Army* (Santa Monica, CA: RAND Corporation, 2015), p.26.

[25] Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Report Prepared for the U.S.-China Economic and Security Review Commission, 7 March 2012, p. 14, 30, http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-066.pdf

[26] Michael Chase and Arthur Chan, *China's Evolving Approach to Integrated Strategic Deterrence* (Santa Monica: RAND Corporation, 2016), p.17, http://www.rand.org/pubs/research_reports/RR1366.html.

[27] Information Office of the State Council of the People's Republic of China, *China's National Defense in 2015*, 26 May 2015, http://eng.mod.gov.cn/Database/WhitePapers/index.htm.

[28] Taylor Fravel, 'China's New Military Strategy: Winning Informationized Local Wars', *The China Brief*, 2 July 2015, https://jamestown.org/program/chinas-new-military-strategy-winning-informationized-local-wars/.

At the same time, China’s foreign policy uses economic leverage and “soft power” diplomacy as primary means of power projection, Beijing has been also actively exploiting concepts associated with strategic information operations to direct influence on the process and outcome in areas of strategic competition. In 2003, the Central Military Commission (CMC) approved the guiding conceptual umbrella for information operations for the People’s Liberation Army (PLA) – the “Three Warfares” (*san zhong zhanfa*). The concept is based on three mutually-reinforcing strategies: (1) the coordinated use of strategic psychological operations, (2) overt and covert media manipulation, and (3) legal warfare designed to manipulate strategies, defense policies, and perceptions of target audiences abroad. Historically, the primary target for China’s information and political warfare campaigns has been Taiwan. Since the 1950s, for example, the Nanjing Military Region’s 311 Base (also known as the Public Opinion, Psychological Operations, and Legal Warfare Base) in Fuzhou City, Fujian Province, broadcasted propaganda at Taiwan through the “Voice of the Taiwan Strait” (VTS) radio. At the same time, China’s information operations attempted to exploit political, cultural, and social frictions inside Taiwan, undermining trust between varying political-military authorities, delegitimising Taiwan’s international position, and gradually subverting Taiwan’s public perceptions to “reunite” Taiwan on Beijing’s terms.

Prior to the 2016 organizational reforms of the People’s Liberation Army (PLA), the strategy of “Three Warfares” was the responsibility for the PLA’s General Political Department- Liaison Department (GPD/LD). In the past, the GPD-LD supported civilian and business platforms working to “promote Chinese culture” abroad such as the China Association for Promotion of Chinese Culture (CAPCC); China Association for Friendly International Contacts (CAIFC); China-U.S. Exchange Foundation (CUSEF), The Centre for Peace and Development Studies (CPDS), External Propaganda Bureau (EPB), and China Energy Fund Committee (CEFC). In doing so, the GPD/LD has been associated with PLA’s military intelligence networks, identifying select foreign political, business, and military elites and organisations abroad relevant to China’s interests or potential “friendly contacts.” In their research, they analyse their position toward China, career trajectories, motivations, political orientations, factional affiliations, and competencies. The resulting “cognitive maps” guide the direction and character of tailored influence operations, including conversion, exploitation, or subversion. Meanwhile, the GPD’s Propaganda Department broadcasts sustained internal and external strategic perception management campaigns through mass media and cyberspace channels to promote specific themes favourable for China’s image abroad – political stability, peace, ethnic harmony, and economic prosperity supporting the narrative of the “China model” (zhongguo moshi).

In Russian strategic thought, a military cyber campaign has been also viewed in a holistic information (cyber) operation context, "waged simultaneously on the digital-technological and on the cognitive-psychological fronts, which skillfully merges military and non-military capabilities across nuclear, conventional, and sub-conventional domains."[29] Contrary to Western perceptions of Russian "hybrid warfare" influenced by Gen. Valery Gerasimov, the current Chief of the General Staff of the Armed Forces of Russia, who published an article in February 2013 on his views on the operational environment and the nature of future wars[30], Russian strategic community has been developing responses to what it perceives as a Western "hybrid warfare" directed against Russia. In this context, Russian concepts of New Generation Warfare (NGW) are not new; they build upon a historical tradition of Soviet-Russian informational (cyber) struggle, which derived from the confluence of three sources: (1) Soviet conceptions of Military Technological Revolution of the 1980s, (2) tradition of "active measures" of denial, deception, disinformation, propaganda, and concealment (*maskirovka*) in the Soviet-Russian operational art, and (3) unique Soviet scientific discipline of cybernetics (*kibernetika*) linking social and natural sciences. [31] The contours of Russian information struggle identify the main battlespace as the mind of the enemy, which means "influence operations" are of strategic importance, including elaborate internal communications, deception operations, psychological operations and well-defined external strategic communications in the cyber domain. Their key aim is to manipulate the adversary's perceptions, shape its decision-making process, and strategic choices, while minimizing the scale of kinetic force. Accordingly, informational struggle can be characterized as *holistic* – merging cyber-technical and cognitive-psychological attacks; *unified* – synchronizing information operations with military and non-military actors, means and other instruments of power; and *permanent* – waged during peacetime and wartime, simultaneously in domestic and external information spheres. [32]

The development of defensive and offensive cyber capabilities, while preparing for long-term confrontation in a hostile environment, is also part of a new "Information Security

[29] Dima Adamsky, 'Cross-Domain Coercion: The Current Russian Art of Strategy', *Proliferation Papers*, vol. 54, IFRI Security Studies Center, 2015, p.10, http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

[30] Valery Gerasimov, 'The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations,' *Voyenno-Promyshlennyy Kurier (VPK) (Military-Industrial Courier),* 27 February, 2013.; Charles Bartles, 'Getting Gerasimov Right,' *Military Review*, January/February 2016, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art009.pdf

[31] Dima Adamsky, 'Cross-Domain Coercion: The Current Russian Art of Strategy', *Proliferation Papers*, vol. 54, IFRI Security Studies Center, 2015, p. 28, http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

[32] Dima Adamsky, 'Cross-Domain Coercion: The Current Russian Art of Strategy', *Proliferation Papers*, vol. 54, IFRI Security Studies Center, 2015, p. 29, http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

Doctrine" signed by President Vladimir Putin on December 5, 2016. The document replaces the 2000 version, addressing new challenges to Russia's national security brought by the diffusion and increasing penetration of information technologies, including foreign cyberattacks and misinformation campaigns - "the capacities to influence [Russian] information infrastructure by a number of countries in pursuit of military objectives."[33] While the new Doctrine views information security at three levels – individual, societal, and governmental, it fully prioritizes national interests and government control in protecting Russia's information sphere.[34] In doing so, it builds on recent measures and new laws that require all Internet service providers (ISPs) to store the data on servers physically located on the territory of Russia; gather the bulk of personal data, keep it for six months and share it with intelligence agencies directly. At the same time, it views information security in an ambiguous context of strategic deterrence – "this can mean the use of information as a deterrent for preventing conflicts in cyberspace. On the other, it can mean deterring conventional strategic threats using military cyber capabilities."[35]

Strategic Competition

In Asia-Pacific, the underlying sources and drivers for cyber and information warfare capabilities are deeply embedded in regional complex security dilemmas: the struggle for dominance by the region's two major powers (China and Japan); the future of Taiwan and the Korean Peninsula; intra-regional competition in territorial disputes in the East China Sea and South China Sea; and perhaps most importantly, the contours of long-term regional strategic competition and rivalry between China, Russia, and the United States. In one school of thought, states pursue the development, acquisition, deployment, and exercising of forces as means to create advantages and influence events or strategic choices of particular competitor.[36] In this context, China, Russia, and the US are in a long-term strategic competition to sustain or prolong the margin of their military-technological superiority or create strategic advantages through military innovation and political influence. The development of cyber capabilities in Asia-Pacific thus proceeds parallel with military-technological innovations – for example, in the research and

[33] Официальный интернет-портал правовой информации, 'Указ Президента Российской Федерации от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации', http://publication.pravo.gov.ru/Document/View/0001201612060002?index=0&rangeSize=1.

[34] Pavel Sharikov, 'What is behind Russia's New Information Security Doctrine', Russia Direct, 19 December, 2016, http://www.russia-direct.org/opinion/what-behind-new-russias-information-security-doctrine.

[35] Pavel Sharikov, 'What is behind Russia's New Information Security Doctrine', Russia Direct, 19 December, 2016, http://www.russia-direct.org/opinion/what-behind-new-russias-information-security-doctrine.

[36] Thomas Mahnken, 'Thinking about Competitive Strategies', in Thomas Mahnken (ed), *Competitive Strategies for the 21st Century* (Stanford: Stanford University Press, 2012).

development of dual-use technologies that enable (1) *perception, processing, and cognition* (i.e. artificial intelligence, cloud computing, robotics, unmanned systems, advanced sensors, big data analytics), (2) *performance and materials* (i.e. quantum computing, autonomous systems, bio-materials), (3) *communication, navigation, and targeting* (i.e. precision position, navigation, and timing, directed energy, electro-magnetic weapons, hypersonics), and (4) *manufacturing, logistics, and supply chains* (i.e. additive manufacturing, 4D printing, simulation and training, computer aided design).[37]

In the US, these efforts are currently conceptualized under the *Third Offset Strategy* that seeks to develop "technologically enabled operational and organizational constructs that provide the joint force an advantage -- primarily at the operational level of war, but also the tactical -- thereby strengthening conventional deterrence."[38] While US defense officials caution that the Third Offset Strategy does not aim at specific peer competitor (i.e. Russia, China), the strategy's underlying assumption is that the global diffusion of advanced military technologies in emerging domains of warfare – space, near-space, cyberspace, and underwater - constraints US forces' the access and freedom of action; the ability to maintain localized air superiority, maritime superiority, space and cyberspace superiority and security, in addition to the ability to conduct cross-domain operations and maneuver in select contested areas.[39]

The Third Offset's top priority investments also include the development of innovative cyber-enabled defense capabilities such as battle management and command and control of a space constellation under threat of attack – led by the newly established Joint Interagency Combined Space Operations Center (JICSpOC).[40] Another major concern for the US military is securing combat support and logistics systems - assets that are critical for rapid global force deployment.[41] On the offensive side, open source references hint at a range of classified cyber-attack techniques conceptualized under the DoD's Advanced Capabilities and Deterrence Panel. These include "non-kinetic missile defenses such as the planned use of cyber-attacks and other electronic warfare means,

[37] T.X. Hammes, 'Technologies Converge, Power Diffuses', Paper presented at RSIS-TDSI Seminar *'Disruptive Defence Technologies in Military Operations'*, Singapore, 29 June 2016, https://www.rsis.edu.sg/wp-content/uploads/2016/08/ER160823_RSIS-TDSI.pdf.

[38] Cheryl Pellerin, 'Deputy Secretary Discusses Third Offset, First Organizational Construct', *Department of Defense News*, 21 September 21 2016, http://www.defense.gov/News/Article/Article/951689.

[39] Terry Morris, Martha VanDriel, William Dries (et al), 'Securing Operational Access: Evolving the Air-Sea Battle Concept,' *The National Interest*, 11 February 2015, http://nationalinterest.org/feature/securing-operational-access-evolving-the-air-sea-battle-12219.

[40] Christian Davenport, 'A Fight to Protect 'the Most Valuable Real Estate in Space', *The Washington Post*, 9 May 2016, https://www.washingtonpost.com/business/economy/a-fight-to-protect-the-most-valuable-real-estate-in-space/2016/05/09/df590af2-1144-11e6-8967-7ac733c56f12_story.html?utm_term=.b3e7fdfa56c4.

[41] Don Snyder, George Hart, Kristin Lynch, and John G. Drew, 'Ensuring U.S. Air Force Operations During Cyber Attacks Against Combat Support Systems', *RAND Research Report*, no. 620, 2015, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR620/RAND_RR620.pdf.

such as electromagnetic pulse attacks, against foreign command and control systems."[42] Advanced military cyber capabilities, both offensive and defensive, also aim at exploiting vulnerabilities in the security, reliability, and integrity of mission-critical command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems – from denial, deception, disruption to subversion to other emerging forms of electronic warfare, including electromagnetic pulse and high-powered microwave weapons.[43]

In China, the strategic competition for the research, development, and acquisition of cutting-edge military technologies, including cyber capabilities that would enable the People's Liberation Army (PLA) to fight and win "informationized local wars" is embedded in the concept of military-civil integration – MCI (*junmin ronghe*, 军民融合). According to the 2015 *China Military Strategy*, "China will work to establish uniform military and civilian standards for infrastructure, key technological areas and major industries, explore the ways and means for training military personnel in civilian educational institutions, developing weaponry and equipment by national defense industries, and outsourcing logistics support to civilian support systems."[44] While the MCI builds upon established principles of civil-military integration (*yujun yumin,*于军于民), which have for over two decades promoted the development of dual-use technologies and combined defense and civilian industrial bases[45], President Xi Jingping has elevated MCI into a national-level strategy:[46] "the integration of civilian and defense development will involve multiple fields and enable economic progress to provide a 'greater material foundation' for defense construction, while the latter offers security guarantees for the former."[47] In this context,

[42] Bill Gertz, 'Pentagon Developing Pre-Launch Cyber Attacks on Missiles', *The Washington Free Beacon*, 14 April, 2016, http://freebeacon.com/national-security/pentagon-developing-pre-launch-cyber-attacks-missiles/

[43] Paul Davis and Peter Wilson, 'Looming Discontinuities in U.S. Military Strategy and Defense Planning', *RAND Occasional Papers*, no. 326, 2011, p.12, http://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP326.pdf.

[44] Information Office of the State Council of the People's Republic of China, *China's National Defense in 2015*, 26 May 2015, http://eng.mod.gov.cn/Database/WhitePapers/index.htm.

[45] Under the principle of *Yujun Yumin* – "locating military potential in civilian capabilities," prioritized in the 2004 Defense White Paper, subsequent Five-Year Defense Plans, as well as in the 2006-2020 Medium- and Long-Term Defense Science and Technology Development Plan (MLP), China embarked on a series of defense industry reforms that would translate into qualitative technological advances for the People's Liberation Army (PLA). See: Information Office of the State Council of the People's Republic of China, *China's National Defense in 2004*, 27 December 2004, http://www.gov.cn/english/2006-02/09/content_183426.htm; Eric Hagt, 'Emerging Grand Strategy for China's Defense Industry Reform,' in Roy Kamphausen, David Lai, and Andrew Scobell (eds.) *The PLA at Home and Abroad: Assessing the Operational Capabilities of China's Military* (Carlisle, PA: U.S. Army War College, 2010), p. 481-484.

[46] "Military-civilian cooperation, as a national strategy, is crucial to national security and the bigger picture of development." Xinhua News, 'Xi Urges Greater Military-Civilian Cooperation for Strong Army', 19 October, 2016, http://news.xinhuanet.com/english/2016-10/19/c_135766754.htm.

[47] Xinhua News, 'China Focus: China Targets Better Integrated Military, Civilian Development', 21 July 2016, http://news.xinhuanet.com/english/2016-07/21/c_135530920.htm

MCI aims to further integrate state-owned defense research, development, and manufacturing enterprises, government agencies under the State Council, universities, and private sector firms in order to advance PLA's military modernization, while supporting China's economic growth.[48]

MCI strategy also relies on foreign acquisition of dual-use technologies, resources, and knowledge in select priority areas identified in long-term defense science & technology plans such as the newly formulated "Defense Science and Technology Industry 2025 Plan" (国防科技工业2025) and the "Made in China 2025 Plan (中国制造2025).[49] These plans represent a follow-on to the "2006-2020 Medium- and Long-Term Plan on the Development of Science & Technology", and "Strategic Emerging Industries Plan of 2010" (战略性新兴产业) that emphasized "Indigenous Innovation" (自主创新) or absorptive capacity to recognize, assimilate, and utilize external knowledge to accelerate the development of China's advanced technologies in both civil and military domains.[50]

According to the 2016 *US Department of Defense Annual Report to Congress*, "China continues to supplement indigenous military modernization efforts through the acquisition of targeted foreign technologies, including engines for aircraft, tanks, and naval vessels; solid state electronics and microprocessors, guidance and control systems; enabling technologies such as cutting-edge precision machine tools; advanced diagnostic and forensic equipment; and computer-assisted design, manufacturing, and engineering."[51] In doing so, the US sees China conducting various forms of cyber espionage,[52] in order to "reduce the costs and lead time" of select PLA's military modernization programs,

[48] Greg Levesque and Mark Stokes, *Blurred Lines: Military-Civil Fusion and the 'Going Out' of China's Defense Industry* (Washington D.C.: Pointe Bello, 2016, http://www.pointebello.com/s/122016_MCF-Report_Pointe-Bello-nzf6.pdf.

[49] Tai Ming Cheung, Thomas Mahnken, Deborah Seligsohn, Kevin Pollpeter, Eric Anderson, and Fan Yang, ''Planning for Innovation – Understanding China's Plans for Technological, Energy, Industrial, and Defense Development,' report prepared for the U.S.-China Economic and Security Review Commission, July 28, 2016, p.120, http://www.uscc.gov/Research/planning-innovation-understandingchina.E2%80%99s-plans-technological energy-industrial-and-defense.

[50] Tai Ming Cheung, 'The Chinese Defense Economy's Long March from Imitation to Innovation', *Journal of Strategic Studies*, vol.34, no. 3, 2011, p.343-344; Scott Kennedy, 'Made in China 2025', Center for Strategic & International Studies, 1 June 2015, https://www.csis.org/analysis/made-china-2025.

[51] Office of the Secretary of Defense, 'Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016,' Department of Defense (2016). Available at: http://www.defense.gov/Portals/1/Documents/pubs/2016%20China%20Military%20Power%20Report.pdf

[52] Jon Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application," In Jon Lindsay, Tai Ming Cheung, and Derek Reveron, eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (New York, NY: Oxford University Press, 2015), p.66.

mitigate technological risks and structural deficiencies in China's defense industries, and bypass long-standing export controls of sensitive military technologies to China.[53]

The issue of cyber espionage has consistently raised tensions in the Sino-US relations. In February 2016, for example, the Director of National Intelligence, James R. Clapper, delivered his annual threat briefing to the Senate Armed Forces Committee noting that China remains engaged in malicious activities in cyberspace against the United States, despite a US-Chinese bilateral agreement to refrain from conducting or knowingly supporting commercial cyber-espionage. "China continues to have success in cyber espionage against the US government, our allies, and US companies….Beijing also selectively uses cyberattacks against targets it believes threaten Chinese domestic stability or regime legitimacy."[54] At the same time, leading US cyber experts have shared concerns over Chinese cyber penetrations of both commercial and government networks.[55] These views are reflected in other influential US government reports such as the Department of Defense's *2015 Annual Report to Congress* on China.[56]

Meanwhile, China's policy makers at the highest levels have refuted these allegations, arguing that the Chinese military does not steal commercial secrets or support Chinese companies which do so. Prior to his state visit to the United States in September 2015, for example, president Xi Jinping said in a written interview with the *Wall Street Journal* that "cyber theft of commercial secrets and hacking attacks against government networks are both illegal; such acts are criminal offences and should be punished according to law and relevant international conventions. China and the United States share common concerns on cyber security."[57] Other Chinese government sources have become more direct in criticizing the US for its 'double standard' – accusing China, while conducting cyber-espionage itself. In particular, China points to the National Security Agency (NSA) cyber-activities against other countries as revealed by Edward Snowden, and views them as a threat to China. In May 2014, the Ministry of National Defense of the PRC issued a statement accusing the U.S. of hypocrisy, "from the 'WikiLeaks' to the 'Snowden' incident,

[53] David Alexander, 'Theft of F-35 Design Data is Helping U.S. Adversaries - Pentagon', *Reuters*, 19 June 2013, http://www.reuters.com/article/usa-fighter-hacking-idUSL2N0EV0T320130619.

[54] James Clapper, 'Worldwide Threat Assessment of the US Intelligence Community', *Senate Armed Services Committee: Statement for the Record* (February 9, 2016). Available at: http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf

[55] James Lewis, 'Asia: The Cybersecurity Battleground,' Statement before the *House Foreign Affairs Committee*, Subcommittee on Asia and the Pacific (July 23, 2013). Available at: http://csis.org/files/attachments/130723_jimlewis_testimony_v2.pdf

[56] Office of the Secretary of Defense, 'Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015,' Department of Defense (2015). Available at: http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf

[57] Charles Hutzler, 'Despite Slump, China's Xi Jingping Pledges Economic Reforms,' *The Wall Street Journal* (September 22, 2015).

the U.S. hypocrisy and double standards on the issue of network security has long been obvious."[58]

Cyber-Enabled Information Conflicts in Regional Security Flashpoints

In East Asia, cyber-enabled information conflicts are increasingly shaping the character of regional security flashpoints: the struggle for dominance by the region's two major powers (China and Japan); the future of the Korean Peninsula; intra-regional competition in territorial disputes in the East China Sea and South China Sea; and long-term regional strategic competition between China and the United States. In particular, every major security issue in East Asia reflects parallel and continuous confrontations in and out of cyber space, and varying cyber and information operations by both state and non-state actors. On one hand, these "hybrid" operations serve as asymmetric means of warfare, providing a range of options that pose relatively lower risks of escalation or without any visible military commitments. The character of asymmetric cyber-attacks, however, may also increase the propensity for offensive and unrestricted character of cyber operations given the prevailing perceptions of lesser risks of detection, the lack of accountability, and the resulting low probability of successful deterrence.[59]

With its outdated, inferior armed forces, and lack of resources to shift the military balance on the Korean Peninsula, for example, North Korea has been relying on nuclear weapons, ballistic missiles, special forces, and cyber capabilities as forms of asymmetric negation strategies to offset specific US-ROK (Republic of Korea) conventional military strengths.[60] Since 2009, North Korea has been attributed to a number of major cyber and electronic warfare attacks, including electromagnetic waves to jam satellite traffic navigation signals in South Korea, distributed denial of service attacks and other forms of cyberattacks on banks and the websites of major businesses and ROK's public agencies including the Presidential Palace (Cheong Wa Dae), National Assembly, and Defense Ministry, and the November 2014 attack against Sony Pictures Entertainment.[61] In a latest major cyber-attack, reported in December 2016, South Korean Ministry of National Defense (MND) attributed North Korea to hacking into ROK's Cyber Command – marking the first time

[58] Ministry of National Defense of the PRC, 'Defense Ministry spokesman Geng Yansheng's Remarks on the US Justice Department sued Chinese soldiers,' *MND Press Release* (May 20, 2014), Available at: http://news.mod.gov.cn/headlines/2014-05/20/content_4510313.htm

[59] Lior Tabansky, 'Basic Concepts of Cyberwarfare', *Military and Strategic Affairs*, vol. 3, no.3, 2011, p.75-92.

[60] Sangho Song, 'N. Korea Bolsters Cyberwarfare Capabilities', *The Korea Herald*, 27 July 2014, http://www.koreaherald.com/view.php?ud=20140727000135.

[61] Sangho Song, 'Korea Vulnerable to Cyberwarfare, *The Korea Herald*, 6 July 2014, http://www.koreaherald.com/view.php?ud=20140706000175.

that the data of South Korea's Cyber Command has been compromised.[62] According to the 2014 ROK Defense White Paper, “North Korea currently operates about 6,000 cyber warfare troops and conducts cyber warfare, including the interruption of military operations and attacks against major national infrastructure, to cause psychological and physical paralysis in the South. The performance of their conventional weapons is also continuously upgraded.”[63]

In particular, North Korea’s cyber operations evolve in the context of “deliberate and organized efforts under the direction of preexisting organizations with established goals and missions that directly support the country’s national strategy.”[64] Pyongyang views the Korean peninsula entrenched in a geopolitical deadlock with the current “correlation of forces” unfavorable to North Korea’s key strategic objective to control and reunify the Peninsula on North Korea’s terms. Under these conditions, Pyongyang aims to gain strategic advantage by pursuing irregular and asymmetric military capabilities, including cyber capabilities, which provide relatively low-cost but highly effective means to exert its influence and provide military coercion without triggering a major armed conflict. At the operational level, North Korea’s principal cyberwarfare organizations – the KPA General Staff Department (GSD) and the Reconnaissance General Bureau (RGB), share different but mutually-supporting responsibilities – GSD bureaus such as the Electronic Warfare Bureau and the Enemy Collapse Sabotage Bureau (Unit 204) are tasked with information and electronic warfare aligned with cyber-attacks to disrupt the opponent’s conventional operations during wartime, while the RGB’s cyber units such as the Bureau 121 conducts offensive and defensive cyber operations, cyber espionage, network exploitation, and cyber-crime activities during peacetime. Accordingly, North Korea’s cyber operations are a part of a “holistic effort on information warfare that incorporates all aspects of affecting information such as electronic warfare, cyber warfare, and psychological operations.”[65]

While the ROK’s core security concerns are more about responding effectively against North Korea’s growing WMD capabilities, the ROK military has been also strengthening its cyber capabilities, both offensive and defensive, as part of a “full-spectrum military

[62] Kyongae Choi, 'N. Korea likely Hacked S. Korea Cyber Command: Military', *Yonhap News*, 6 December 2016, http://english.yonhapnews.co.kr/news/2016/12/05/0200000000AEN20161205010451315.html.

[63] Republic of Korea Ministry of National Defense, *2014 Defense White Paper* (Seoul: MND, 2014), p.27, http://www.mnd.go.kr/user/mnd_eng/upload/pblictn/PBLICTNEBOOK_201506161152304650.pdf.

[64] Jenny Jun, Scott LaFoy, and Ethan Sohn, *North Korea’s Cyber Operations: Strategy and Responses* (Washington D.C.: Center for Strategic and International Studies, 2015), p.5, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf.

[65] Jenny Jun, Scott LaFoy, and Ethan Sohn, *North Korea’s Cyber Operations: Strategy and Responses* (Washington D.C.: Center for Strategic and International Studies, 2015), p.51, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf.

readiness posture" against a range of potential North Korean provocations.[66] In 2011, the MND published a cyber-defense strategy – the *Master Plan for Defense Cyber Policy*, which emphasized four key policy directives: adapting South Korea's laws to enable cyber operations; integrating cyber and physical operations in a military doctrine - the Joint Cyber Operations Manual; establishing ROK Cyber Command under the Joint Chiefs of Staff office; and creating early warning and crisis management mechanisms for responding to cyber crises.[67] In 2016, South Korea's MND agreed to enhance civil-military cooperation in the cyber domain, including joint programs with the Ministry of Science, IT, and Future Planning and the National Intelligence Service (NIS) to create a possible cyber reserve force, and closer coordination of intelligence CCTV border monitoring, joint response to GPS jamming, and a special warfare-centered combat skills augmentation plan. Ultimately, South Korea's cyber capabilities have evolved in the strategic framework of the US-ROK alliance with joint programs developing artificial intelligence-based technologies to counter a range of cyber threats. [68]

The use of cyber means as political instruments of warfare is increasingly reflected also in the ongoing territorial disputes over the South China Sea. In July 2015, as the Permanent Court of Arbitration in The Hague conducted a hearing on the South China Sea Arbitration brought by the Philippines against China, the Court's website went offline. The site was also infected with malware, leaving visitors interested in the case at risk of data theft. Based on the analysis of the software and infrastructure used, the attack's origin was attributed to China.[69] The incident follows a pattern of spiking cyber activities relative to the rise tensions in the South China Sea. This is evident, for example, in the rise of cyberattacks on Vietnamese targets as China moved an exploration oil rig into contested waters in mid-2014.[70] On July 29, 2016, a major cyber-attack targeted Vietnam's two largest airports and Vietnam Airlines – the flight screens at the airports showed messages critical of Vietnam's claims to the South China Sea, and the airport's

[66] Republic of Korea Ministry of National Defense, *2014 Defense White Paper* (Seoul: MND, 2014), p.18, http://www.mnd.go.kr/user/mnd_eng/upload/pblictn/PBLICTNEBOOK_201506161152304650.pdf.

[67] Republic of Korea Ministry of National Defense, *2014 Defense White Paper* (Seoul: MND, 2014), p.18, http://www.mnd.go.kr/user/mnd_eng/upload/pblictn/PBLICTNEBOOK_201506161152304650.pdf.

[68] Chung Min Lee, 'Enhancing US Power Projection', In: Patrick Cronin (ed.) Breakthrough on the Peninsula: Third Offset Strategies and the Future of Defense of Korea (Washington D.C.: Center for New American Security, 2016), p.70, https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-BreakthroughonthePeninsula-Finalb.pdf

[69] David Tweed, 'China's Cyber Spies Take to High Seas as Hack Attacks Spike', *Bloomberg*, 16 October 2015, https://www.bloomberg.com/news/articles/2015-10-15/chinese-cyber-spies-fish-for-enemies-in-south-china-sea-dispute.

[70] John Boudreau and Mai Ngoc Chau, 'Spyware Deluge Hits Vietnam Sites Amid South China Sea Spat', *Bloomberg*, 10 August 2016, https://www.bloomberg.com/news/articles/2016-08-09/spyware-deluge-attacks-vietnam-sites-amid-south-china-sea-spat

sound system broadcasted anti-Vietnamese and Philippines slogans.[71] A Chinese patriotic hacktivist groups 1937cn claimed responsibility for the attack.[72]

Implications for Singapore

As conflicts move into the cyber and information domains, there is an ongoing debate on the magnitude and impact of cyber and information operations on East Asian security. On one hand, sceptics argue that there are serious limitations with regard the use of cyberspace for political purposes, particularly at the higher end of the conflict spectrum in East Asia. In this view, cyber-enabled information operations alone cannot strengthen capabilities for coercion or deterrence – they do not transform regional power structures, do not replace the military capabilities of the most advanced powers in the region, and ultimately, have a limited utility to achieve desired political outcomes. Consequently, they may not provide significant strategic advantages in achieving political objectives. The prevailing view, however, is that regional conflicts and potential flashpoints in Asia Pacific already transcend into the cyber and information domains and have significant political ramifications. Indeed, the confluence of varying cyber strategies and information operations capabilities in the broader context of regional power transitions shapes the direction, pace, character of military change in Asia Pacific.

First, cyber-enabled information operations enable and reinforce strategic ambiguity in terms of effects, sources, and motives, and therefore can be used to deny or create political outcomes without visible military commitments. Second, the deepening systemic interdependencies brought by information technologies in nearly all aspects of governance (i.e. energy systems, communications, water, transportation, finance, etc.) render traditional conceptions of deterrence and defense vulnerable to strategic surprises - asymmetric forms of information and cyberwarfare. Third, cyber-enabled information operations – defensive, offensive, and intelligence-driven increasingly serve as a key enabler and force-multiplier of kinetic operations – enabling actions, capabilities, and effects of land, sea, air, and space operations in all physical domains. Fourth, cyber operations are synonymous with information operations – in the ability to penetrate target audiences in real time. For example, crafting messaging campaigns to go “viral” to shape

[71] BBC News, ‘South China Sea: Vietnam Airport Screens Hacked’, 29 July 2016, http://www.bbc.com/news/world-asia-36927674.

[72] VnExpress, ‘Cyber-terrorists Attack Flight Info Screens at Vietnam’s 2 Major Airports,’ 29 July 2016, http://e.vnexpress.net/news/news/cyber-terrorists-attack-flight-info-screens-at-vietnam-s-2-major-airports-3444504.html

perceptions, narratives, and create cognitive effects in which online behavior has offline consequences and vice versa. Fifth, cyber-enabled information warfare capabilities evolve parallel with military-technological advances such as electronic miniaturization, additive manufacturing, nano-technologies, artificial intelligence, space capabilities, and unmanned systems that alter the character of future warfare. Given the varying levels of socio-economic development, defense resource allocation, and military-technological trajectories, there will also considerable variation in the adaptation of cyber capabilities. The variance will also reflect different strategic cultures and doctrinal conceptions on the use of cyber means as instruments of warfare.

Taken together, comprehensive cyber capability requirements will increasingly shape strategic choices in Asia Pacific - defense planning, management, and technological priorities, propelling the need for strategic and operational adaptation and innovation to prepare for, fight, and win new types of wars. The challenge for Singapore is to be able to adapt to these potential changes to the character of war. The reality is that Singapore's security paradigm remains relatively unchanged, in terms of its current doctrines and strategies. However, in a context where the battle space is crowded with both legally constituted combatants and non-combatants using cyber-enabled information operations, this will present new set of challenges to Singapore.

Recommendations:

- Singapore needs to explore the nature of the evolving strategic competition in East Asia. In this context, Singapore may become vulnerable to other non-traditional emerging threats, particularly political and hybrid warfare. As conflicts evolve parallel in the cyber and information domains, the centers of gravity are also going to shift. The value and more importantly, the accuracy and reliability of strategic information relevant for the situational awareness and function of the nation state as a system will become even more important with the increased dependence on cyberspace.

- As more governments, intelligence agencies, military organisations as well as non-state actors invest in developing cyber / information warfare 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. The resulting "cyber-kinetic conflicts" will evolve parallel with technological changes – e.g. the introduction of next generation of robots, artificial intelligence, and remotely controlled systems that will continue to alter the character of future warfare.

- The character of hybrid conflicts in the regional “gray zones” may also likely reflect low-level intensity conflicts in “peripheral information/influence campaigns”, rather than high-end conflicts – given the considerable escalatory risks. Under the changing character of conflict, Singapore and the SAF will likely have to redefine its objectives necessary to achieve “victory.”

- These issues highlight the strategic significance of the 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. Online activities and behaviour will have increasingly offline consequences, and vice-versa.