Warfare Evolved:

Disruptive Military Technologies and their Geopolitical Implications

Geopolitical Monitor
Intelligence Corp.

Written by Alessandro Gagaridis, 2020

Geopoliticalmonitor Intelligence Corp.
5700-100 King Street West, Toronto, Ontario, Canada M5X 1C7
www.geopoliticalmonitor.com

Table of Contents

Quantum Encryption

Progress in quantum technologies is poised to have a considerable impact on future warfare. Apart from quantum radars – which have the potential to make stealth vectors and jamming techniques obsolete – the application of quantum physics may also have deeply disruptive effects in other fields. Quantum-based encryption, communications and computing are expected to revolutionize how information is elaborated and exchanged by drastically increasing calculating power and security. This would complicate intelligence-gathering activities, but would also turn the material infrastructure supporting these technologies into a primary target for enemy strikes. China seems to be leading the way in this emerging technology that involves cutting-edge research programs and sophisticated satellites orbiting around Earth, but other powers are also involved and the outcome of this competition, which will have serious consequences in the decades to come.

SECURING INFORMATION: THE PHYSICS OF QUANTUM ENCRYPTION

Normally, information security is ensured by using complex algorithms to encrypt data and make them unintelligible to eavesdroppers. But with enough time and computational power, these cyphers can be cracked, thus allowing intercepted messages to be read. Technological progress (notably in quantum computers) will bring ever greater calculation power, which will have the effects of making it easier to break cyphering codes and reducing the effectiveness of traditional encryption.

A potential answer to this challenge comes from quantum physics itself. The fundamental point is that sub-atomic particles can be influenced so that they take on one of two different states. When the particle is observed, it takes only one of them. But when it is *not* observed, it exists in a particular condition called ‘superposition,’ meaning that its status is a combination of the two. Or in other words: it holds both statuses at once. The simple acts of observing it will end the superposition and force the particle into taking on one of its two possible states. Another peculiar and counter-intuitive property of quantum physics is that two particles can be ‘linked’ so that they take on and preserve the same state, even if they are considerably distant from one from the other. This is a phenomenon known as ‘entanglement.’

These innate properties can be exploited to store, carry, and deliver information – all in a perfectly secure manner, thanks to a process called quantum key distribution (QKD). Everything starts with the generation of a pair of ‘keys’ encrypted using entangled photons. These keys are employed to cypher the transmitted message and then convert it back into a readable form. In practice, this is achieved by transmitting the photons (and the information they carry) in the form of a laser beam. The first experiments did this via optical fibers, but it was soon discovered that they were not an

adequate vector because they absorbed the signal, thus causing the entanglement to break at a relatively short distance, resulting in a loss of information. To solve the problem, a chain of quantum repeaters was created to receive and retransmit the message. Another alternative would be to use satellites, a process that requires great precision though it's more effective since the signal can be transmitted unaltered to and from Earth across the vacuum of space (even though it could be affected when traversing the atmosphere). In any case, the superposition of the photons guarantees the transmission's security: if a third party attempts to intercept (and therefore observe) the message, the quantum status will immediately change. This will not only modify the ciphering keys, thus making the message impossible to decrypt, but will also be noticed by the users who will then abort the communication attempt or alter the message.

This revolutionary method of encrypted communication has been successfully tested by China in 2018 via the Quantum Experiments at Space Scale (QUESS) program, which employed the Micius (Mozi) satellite to successfully enable a video call between Beijing and Vienna.[1] This fist-time event caused a sensation around the world, not only as a scientific breakthrough but also because of its security implications – even more because it suggests that China is ahead of all other powers in the critical domain of quantum technology.

THE EFFECTS ON INTELLIGENCE

If quantum encryption lives up to its billing and is fully developed along with the necessary support infrastructure, the technology will be a game-changer in the field of intelligence-gathering.

Technically known as signal intelligence (SIGINT), the interception and decryption of messages is a major source of information used by governments to collect data on rivals and allies alike. As an example, the US National Security Agency (NSA), which is responsible for SIGINT, is currently America's largest intelligence organization and its world-spanning activities were revealed in 2013 following the disclosure of classified documents by former CIA employee Edward Snowden. But the introduction of quantum secure keys would hugely complicate its task, as traditional interception would become virtually impossible, leaving SIGINT agencies no other choice but to focus on less secure channels (which would reasonably be used for low-importance exchanges) or to obtain the messages from alternative sources – both of which are also slower solutions. Without this invaluable source, information collection could be severely undermined, and with it the overall quality of intelligence analyses upon which governments and military planners (should) rely on to determine the state's foreign and security policies.

[1] https://www.technologyreview.com/2018/01/30/3454/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/

This would inevitably push rivals to seek alternative sources of intelligence to circumvent the quantum encryption wall. While all techniques would be exploited, the most likely consequence would be a revival of the human factor into intelligence collection. The recruitment and management of undercover agents among officials working in key agencies (like foreign ministries or military headquarters) has always played a key and irreplaceable role; but it has partially lost its importance in the past few decades of mass communication due to the (over)reliance on intercepts. But this domain (known as human intelligence, or HUMINT) will re-emerge as a fundamental resource if quantum encryption scales back the role of SIGINT. As a matter of fact, other methods like imagery intelligence (IMINT) or measurement and signature intelligence (MASINT) are greatly useful for assessing the target's capabilities, but they are of little use for inferring intentions – which is paramount in intelligence analysis – whereas HUMINT can provide extremely valuable information in this regard.

Yet this will not be sufficient to completely compensate for the loss of intercepted messages, as recruiting a covert agent is a long, complex, and risky endeavour. Moreover, the consequences on state behaviour will largely be influenced by whether quantum encryption will be used by one or both powers involved in the mutual intelligence competition.

THE STRATEGIC IMPACT OF QUANTUM ENCRYPTION

The first scenario to consider is the asymmetric one, where a state uses quantum encryption and another does not. This would put the former one step ahead of its rival: it would be able to conduct its most secret activities (diplomacy, intelligence gathering, development of new weapons systems, military operations and even surprise attacks) with much less concern of being discovered, possibly to the point of becoming emboldened into committing risky actions. If this state were also capable of intercepting and cracking the other's communications, then it would possess a decisive advantage allowing it to outmaneuver its opponent, who – unable to intercept the quantum-encoded messages – would be working with far less information to evaluate the intentions of the first state, possibly leading to serious misinterpretations and miscalculations. This could be particularly problematic in the event of a crisis, where urgency requires a rapid and accurate assessment of the situation.

If both states were to use this new technology, the result would be a strange stalemate where both sides would be bolstered by their own information security but uncertain over the other's intentions. In this context, the risk of erroneous interpretations becomes even greater as it involves both parties; and the intelligence advantage will belong to the power capable of better exploiting other techniques (notably HUMINT).

Yet, the consequences are not limited to intelligence operations, but also extend to the military level. First, quantum encryption will make it harder for the opponent's military

planners to prepare for an armed confrontation due to less available information. But this will also mean that the infrastructure supporting quantum communications will become a primary objective for any attack (and probably in an initial strike) in an attempt to deprive the enemy of its advantage. Here, much depends on how the network will be built. Satellites appear to be the best option; not only because they enable long-range transmissions, but also because they potentially allow to send messages to distant naval forces. The alternative is to build a network of quantum repeaters, but this presents multiple problems: It is limited to ground transmissions and the destruction of a single station would break the chain thus making communications impossible. Moreover, ensuring adequate protection of the whole grid would be complicated and expensive. Therefore, this solution is probably adequate only for relatively small but advanced states; whereas vast countries will opt for satellites. Yet, while shooting down an orbiting object is not easy, defending it is even more challenging and powers like the US, China and Russia have successfully tested anti-satellite (ASAT) weapons. As a result, quantum communication satellites will likely be destroyed early after hostilities commence, meaning that (unless effective solutions to protect satellites are developed) the military value of this new technology will be limited to intelligence-gathering in peacetime and in the preparatory phase to war.

The aforementioned QUESS project suggests that China is currently leading the way in quantum encryption, but the United States is doing its best to catch up. Washington has been interested in the application of quantum technologies (not limited to encryption) since the mid-90s, and began providing funding for research in the field in the FY2008 budget.[2] Quantum information science was included in the broader National Strategic Computing Initiative in 2015 and the Trump administration created a specific committee responsible for it in August 2019. Other actors involved in quantum technology are the EU, the UK, and Canada. Still, the United States and China remain the main players and it is possible that they will both develop quantum encryption in the coming years, thus reaching the kind of stalemate described above. How this would affect international stability is uncertain, as much depends on how successful other forms of intelligence are; but in case of a crisis the mutual impossibility to recur to SIGINT for determining the opponent's stance may result in dangerous miscalculations. Considering the mounting tensions and the number of potential flashpoints (Taiwan, the Senkaku/Diaoyu, the South China Sea, to name a few), this is a risk worthy of serious consideration, as history shows time and time again that intelligence failures can change the destiny of entire nations.

[2] https://crsreports.congress.gov/product/pdf/R/R45409

Hypersonic Missiles

Hypersonic missiles are a new category of weapons which have sparked intense debate among security experts. Capable of travelling over five times the speed of sound (Mach 5), and of performing evasive maneuvers mid-flight, they are considered practically impossible to intercept using conventional missile defense systems. Adding that in some cases they can carry nuclear warheads, it is immediately clear why they have caused so much concern in regard to their impact on the global strategic equilibrium. The world's leading military powers (the United States, China, and Russia) and other states are working on their development. Even though their specific technical characteristics and actual performance remain shrouded in secrecy, hypersonic weapons are poised to become an integral part of future warfare, with noteworthy implications in military and international terms.

HYPERSONIC MISSILES: THE CURRENT STATE OF THE ART

By definition, hypersonic missiles are vectors capable of reaching speeds equal or superior to Mach 5. There are two sub-types of systems. The first is hypersonic glide vehicles (HGVs), which are launched by ballistic missiles and separate from them in flight to glide at hypersonic speed toward their target; the second is hypersonic cruise missiles (HCMs), which are fired like conventional cruise missiles and use scramjet engines to reach the required speed. In both cases, their sheer rapidity combined with the ability to perform complex evasive maneuvers makes interception a nearly-impossible challenge. As of today, no missile defense system is considered capable of intercepting hypersonic vectors. The United States has explored various anti-hypersonic solutions, but they are still at an early stage of development. Accordingly, no effective defenses exist today against hypersonic strikes; and even though progress may be made in the future, interception will remain a daunting technical challenge, especially in the case of a large-scale attack. Moreover, the fact that hypersonic systems can be armed with nuclear warheads elevates this technical problem to the level of strategic deterrence. Unsurprisingly, the United States has paid particular attention to the development of hypersonic missiles, monitoring both progress made by its own programs as well as those of competitors and allies, as shown by a recent report by the Congressional Research Service.[3]

Russia and China are developing hypersonic weapons in the context of their anti-access / area denial (A2/AD) strategy designed to keep US forces far from their territory and make it impossible for them effectively operate nearby. According to this logic, hypersonic missiles would be used to threaten US carrier battle groups, forward bases, logistical infrastructure, etc. In addition, both regard hypersonic vectors as a

[3] https://fas.org/sgp/crs/weapons/R45811.pdf

countermeasure to overcome US anti-ballistic missile defenses, which in their opinion undermine the nuclear balance by (theoretically) allowing the US to launch their nuclear weapons without fear of retaliation. Owing to their ability to bypass existing defenses, hypersonic missiles would deprive America of its perceived advantage and restore the traditional equilibrium based on mutually assured destruction (MAD).

China has developed a single hypersonic weapon, the DF-ZF (previously called WU-14). This HGV is believed to have a range of 2,000 kilometers and a top speed of Mach 10, and is mainly conceived as an anti-ship 'carrier killer' weapon. China has not clarified whether it will be nuclear-capable or not, but has allegedly tested ballistic missiles for its launch, notably the DF-21D. The weapon may become operational before the end of this year. US sources also claim that China tested a Mach 6 hypersonic vehicle called Xing Kong 2 ('Starry King 2') in 2018, but there is little info on this system.

For its part, Russia seems to be leading the way in the deployment of hypersonic systems. The Avangard (Project 4202 / Yu-74) is a nuclear-capable HGV which entered into service in 2019. With a range of at least 6,000 kilometers, it is equipped with electronic countermeasures, it can perform evasive maneuvers and it can allegedly reach Mach 20; even though this may well be an exaggeration. The 3M22 Tsirkon (Zircon) cruise missile has an estimated range between 400 and 1,000 kilometers and a speed between Mach 6 and 8. It is primarily conceived as an anti-ship weapon fired by naval and air units. The Kh-47M2 Kinzhal ('Dagger') is an atypical system, since it is neither an HGV nor an HCM but rather a hypersonic ballistic missile. With a range of 2,000 kilometers, it can reportedly reach Mach 10. It can carry a nuclear payload and strike ground and naval targets alike. It is expected to become operational in 2020.

The US started developing hypersonic weapons as a possible implementation of the Conventional Prompt Global Strike (CPGS) concept, meant to enable American forces to hit any target in the world within one hour. Dating back to 2008, it was revived to counter China's and Russia's A2/AD strategy by enabling US forces to strike sensible targets like Command, Control, and Communication (C3) centers, military bases, logistical nodes, critical infrastructures and other strategic facilities to undermine the enemy's warfighting capabilities.

Currently, the US has three hypersonic missile programs. First comes the Navy-led Conventional Prompt Strike (CPS), meant to equip a Virginia-class submarine with HGVs. This vector is also the basis for the Long-Range Hypersonic Weapon (LRHW) of the Army, aimed at developing a land-based mobile vector with a range of 2,200 kilometers. Lastly, the Air Force is developing the AGM-183 Air-Launched Rapid Response Weapon (ARRW), smaller in size and meant to equip B-52 strategic bombers. It is important to note that, according to official declarations, none of these programs are on-track to develop nuclear-capable vectors.

Other powers are developing hypersonic weapons. Australia is cooperating with the United States on the Hypersonic International Flight Research Experimentation (HIFiRE) program, which resulted in several tests of both HGVs and scramjets. Japan is also working on both HGVs and HCMs; the former comes in anti-carrier and area suppression variants and should be deployed between 2024 and 2028. India has been cooperating with Russia on the BrahMos II HCM, and some reports indicate it is also developing an indigenous system of the same type. France has also sought Russian collaboration on hypersonic systems, and is modifying its ASN4G cruise missile to reach hypersonic speeds under the V-max (Experimental Maneuvering Vehicle) program. The new weapon is possibly meant for nuclear strike. Germany tested the SHEFEX II HGV in 2012, but the government has apparently reduced funding for the program. Finally, other countries have experimented hypersonic technologies, but apparently with no military intent. These include South Korea, Israel, and Iran. It is notable that most of these countries are advanced economies with considerable military concerns, in several cases involving China.

THE STRATEGIC IMPACT OF HYPERSONIC MISSILES

The first concern arising from the development and deployment of hypersonic systems is their effect on the nuclear balance. The argument advanced by Russia and China that hypersonic vectors restore equilibrium thanks to their ability to penetrate US missile defenses (that they consider destabilizing) is theoretically valid, but in practice is much weaker. While hypersonic systems are currently impossible to intercept, ordinary missiles are also difficult to destroy in flight and a mass attack would be equally unstoppable. As such, Russia and China's argument seems more motivated by the need to justify their hypersonic programs, which are to be interpreted in an A2/AD logic. On the opposite side, many believe that hypersonic systems have destabilizing effects due to the impossibility to ascertain whether they carry conventional or nuclear payloads (ambiguity). Yet, this problem is not unique to hypersonic systems, as there are numerous traditional ballistic and cruise missiles affected by the same problem. Therefore, hypersonic missiles do not bring significant changes to nuclear attack capabilities and rather than nuclear vectors they seem mainly conceived as conventional weapons to deliver rapid strikes to critical targets. Accordingly, it can be concluded that they do not have sensible destabilizing effects *per se* and do not make war more likely.

However, in case of a crisis between great powers sparked by external factors, they may favor an escalatory logic. In such conditions marked by high levels of stress caused by a (perceived) imminent armed threat to vital national interests that leaves little time for response, state-to-state communication deteriorates and decision-makers employ mental shortcuts to quicken their choices, thus making the decision-making process less rational. Under such circumstances, each side may either be tempted to employ hypersonic missiles to launch a rapid and (expectantly) debilitating first strike to

gain a decisive advantage or to employ its hypersonic assets for a preemptive attack to prevent the opponent from doing so. This would result in a 'shoot first or lose it' logic that may lead to an unintended, and possibly nuclear, escalation. In short, hypersonic systems carry the risk of making a crisis more acute, with potentially catastrophic consequences.[4]

As hypersonic systems exit from the experimental phase and become operational, in the short-medium term they will remain the prerogative of advanced countries possessing the necessary resources, technical infrastructure, and know-how. Yet, they will have to be taken into account by military planners. If current expectations are met, they will become powerful tools in state military arsenals, but they will also raise the risks of escalation in the event of a crisis. Therefore, their employment should be carefully assessed and should be governed in a crisis management rather than a warfighting logic to avoid an escalation that may degenerate into a major conflict.

[4] http://www.strategikos.it/files/A.-Gagaridis_The-Strategic-Implications-of-Hypersonic-Missiles.pdf

Quantum Radar

When it was first introduced by the US armed forces toward the end of the Cold War, stealth technology represented a major shift in the conduct of military operations. Low radar observability – a more appropriate term for 'stealth' – allowed American aircraft to safely penetrate into heavily defended areas without being detected by enemy sensors; and it demonstrated its operational value for the first time during the 1991 Gulf War. It then became an integral part of US military operations, one that was gradually applied to other platforms, including ships. While today it is no longer a US monopoly, since other powers like Russia and China have also deployed hardware with purported low-observability features, the technology remains the exclusive domain of advanced militaries and provides a significant operational advantage.

New experimental technologies, however, hold the potential to change the status quo. A new kind of sensor, called 'quantum radar,' holds the promise of detecting stealth platforms. While this technology is still in its early stages and currently presents notable technical limitations, if successful it could usher in the next chapter in the everlasting dialectic between defense and offense in warfare.

WHAT ARE QUANTUM RADARS?

The first step to assess the potential strategic impact of quantum radars is to understand how they work and how they differ from traditional models.

'Radar' is actually an acronym for 'radio detection and ranging,' a term which reveals its basic functioning principle. Radars emit radio waves that, when they hit an object, are reflected back to the source. By analyzing this return signal, radars are able to detect and track the object. To avoid this kind of tracking, there are two possible solutions. The first is jamming, which means producing a signal in the same wavelength as the radar to interfere with it so that it cannot distinguish the return signal from the spoofing emission, thus 'blinding' it. The second is using stealth systems which exploit design features like radar-reflecting shapes and radar-absorbent materials to reduce their radar cross-section (RCS, the amount of radio energy reflected to the source) and render them harder to detect. Even though no stealth platform is completely 'invisible' to radar, as sensors operating in the very high / ultra frequencies (VHF / UHF) band can successfully detect a low-RCS object, this remains a complex endeavor that does not result in a sufficiently precise localization that allows for targeting.[5]

The functioning principle of quantum radars is different. Such systems exploit a particular physical property known as quantum entanglement. When two particles are

[5] https://www.defenceaviation.com/2016/05/how-to-detect-stealth-aircraft.html

entangled, they have the same quantum state and any change in the status of one particle results in a parallel change in the status of the other, even if the they are considerably distant from one another. The quantum radar exploits this property by generating a visible light beam of entangled photons which then splits in two. One half is converted into the microwave band without changing its quantum state and is then emitted by the radar. When the signal hits an object, it is reflected back to the source and converted back to the visible wavelength in order to be compared with the other half of the original beam. Since the quantum state of its particles changed when it collided with the object, the system can detect its presence by observing the differences in the quantum status of the particles present in the two beams and by filtering out those from other sources. A properly-functioning quantum radar would therefore make both jamming and stealth technology useless. Since the jamming system cannot know the quantum state of the radar signal, the characteristics of the spoofing emission will not match and will automatically be ignored. As for stealth platforms, they would still retain their ability to disperse most of the incoming radar signal, but a small part – not sufficient to be detected by conventional radars – will still come back to the source and the observation of changes in the particle's quantum status will result to detection.

Naturally, quantum radars also have their limits. Apart from the fact that they are an experimental technology that needs to be significantly perfected before becoming operational, the main problem lies in their limited range. As a matter of fact, particles lose their entanglement properties at some point due to a phenomenon called quantum decoherence, meaning that quantum radars also lose their ability to detect targets. In 2015, a study concluded that the effective range of quantum radars would be under 7 miles, but the following year a Chinese team claimed to have manufactured a quantum radar of 61 miles of range.[6] While the ability to detect stealth platforms at such distance would still be a considerable feat, it remains much lower than the range of conventional radars. Nevertheless, the prospected introduction of quantum radars in the years ahead may have deep consequences in both military and geopolitical terms.

QUANTUM RADARS: THREE POSSIBLE SCENARIOS

Given the importance of stealth systems in the US military, any power determined to counter its superiority would be interested in quantum radars. As of today, China seems to be leading the way in the field; but the same logic also applies to Russia. Quantum radars would represent a significant enhancement to their anti-access / area denial (A2/AD) strategy conceived to prevent US forces from operating close to their territory. As stealth technology and electronic warfare (EW) techniques such as jamming played a central role in US military operations to penetrate into heavily-defended environment to strike the enemy's command & control (C&C) centers and critical logistical infrastructures, quantum radars would significantly affect the attack capabilities of US

[6] https://spie.org/news/quantum-radar?SSO=1

forces. At the same time, the low range of quantum radars also limits their value as anti-stealth solutions; even though sensor fusion – the sharing of data between different platforms to have a greater view of the battlespace – could offset this problem at least to a certain degree. If quantum radars were able to send detailed enough data on the position (including altitude for aircraft), speed and direction to missile launchers, the latter could use the information to guide their weapons to the target; but this solution presents its own technical challenges.

Depending on the cost and capabilities of quantum radars, three theoretical scenarios are possible, which may coincide with different phases of their development.

If they will turn out to be highly expensive and limited-range systems, as is likely over the short term, they will hardly have any operational value, as enemy stealth platforms would be able to engage their target with long-range standoff weapons well before entering into the quantum radars' detection zone.

If their cost will diminish without significant improvements to their range (possible medium-term scenario), quantum radars will probably be deployed to form dense' grids' of networked sensors to ensure an extensive coverage at least over sensitive target-rich areas. Even though it would complicate the C&C structure of the defenders, this kind of scenario would also present significant challenges to the attacker due to the difficulty of locating and neutralizing a large number of radars and thus disrupting the grid's efficacy. This would be a time-consuming and resource-intensive endeavor, which may be simplified only with accurate intelligence on the location of the individual stations (which would not be easy to obtain) or possibly by using drone swarms to carry out a complex search & destroy operation.

Finally, in the long term the detection range of quantum radars may increase, resulting in a similar use as conventional radars; with the cost influencing only the number of stations deployed. By ensuring detection of enemy aircraft or surface ships over whole regions (for instance the South China Sea), this would have deep strategic consequences. Another possible implication of long-range but low-cost systems would be their miniaturization, allowing them to be mounted on mobile ground vehicles, fighter planes, and so on. This would provide anti-stealth and anti-EW capabilities to expeditionary forces and may potentially lead to a proliferation and a 'normalization' of quantum radars that would significantly change warfare.

THE STRATEGIC IMPLICATIONS OF QUANTUM RADARS

These are of course archetypical scenarios, and reality is likely to take in-between forms also depending on the user's specific strategic environment. Yet, they allow to make some predictions on the impact of quantum radars on international stability. Thanks to their ability to ignore RCS-reducing features and jamming techniques, they would make

it much harder for an attacker to launch a surprise attack with the intent of debilitating its adversary. By reducing the appeal of such an escalatory move, quantum radars would therefore have a stabilizing effect. Yet, warfare is a dialectic process where any advance in defense results in efforts to circumvent it.

To bypass China's and Russia's A2/AD 'bubbles' that quantum radars create alongside other systems, the US will reasonably place greater emphasis on submarines, which can be neither detected by radars (as long as they stay submerged) nor hit by the majority of missiles (though there are examples of anti-submarine missiles); even though another quantum-related technology – namely quantum magnetometers known as superconducting quantum interference device, or SQUID – may offset the benefits of this solution. Unsurprisingly, China seems determined to develop this technology as well.[7]

Hypersonic weapons are another solution since they are nearly impossible to intercept and could be used to neutralize quantum radars (as well as other critical targets); but this may have destabilizing effects by triggering a 'shoot first' dynamic where the US would be tempted to use them to quickly overcome Chinese/Russian defenses and the latter would consider a preemptive hypersonic strike out of fear of being the victims of one.[8] In this sense, quantum radars may indirectly have destabilizing effects; but this is mainly the consequence of hypersonic missiles themselves, also because their influence on the decision to launch a hypersonic first strike would be limited by the fact that, to be effective, such an attack would require complete and accurate intelligence on the location of the quantum radars to be targeted, which is hard to obtain and would require many missiles (especially in the 'grid' scenario described above, which implies a large number of stations to destroy). On this basis, quantum radars will probably have a globally stabilizing effect; but much depends on their actual capabilities and the specific strategic environment where they will be deployed.

To conclude, quantum radars represent a promising technology with the potential to significantly transform warfare in the 21st century by making stealth technology and jamming obsolete in hypothetical great power conflicts. Yet, for the time being they remain experimental systems that are still far from reaching operational use; and as with all new technologies, a considerable margin of uncertainty remains, meaning that only time will tell how quantum radars will affect warfare in the decades ahead.

[7] https://nationalinterest.org/blog/buzz/no-more-stealth-submarines-could-quantum-radar-make-submarines-easy-track-and-kill-54547

[8] http://www.strategikos.it/files/A.-Gagaridis_The-Strategic-Implications-of-Hypersonic-Missiles.pdf

Drone Swarms

Unmanned systems with a variable degree of autonomy, generally known as ‘drones,’ have become commonplace in the world’s advanced militaries. In their various aerial, maritime, and ground forms, these vehicles are used to perform a wide spectrum of roles. Yet advances in new technologies such as artificial intelligence (AI), robotics, and data fusion may revolutionize their employment by enabling large numbers of drones to operate in a coordinated and reactive manner. If fully developed, this concept – known as ‘swarming’ – could have profound tactical and strategic effects; possibly to the point of changing the nature of warfare in the 21st century.

THE CURRENT STATE OF DRONE WARFARE

Today, unmanned systems of different types are used by the militaries of various countries. Here it is necessary to make some important distinctions. First, even though flying platforms (unmanned aerial vehicles, UAVs) are the most common and the ones that are primarily associated with the term ‘drone’ in the collective imagination, they not the only kind of unmanned systems in use. In fact, there are also land-based systems (unmanned ground vehicles, UGVs) and naval platforms, which are in turn divided into two further sub-categories: unmanned surface vehicles (USVs) and unmanned underwater vehicles (UUVs). Second, not all platforms possess the same level of autonomy. Most are actually remotely piloted systems, but there are also fully autonomous drones capable of functioning without the (direct) intervention of human operators; one example being the US Navy’s experimental X-47B. Finally, not all drones can engage targets with weapons. While there are many examples of remotely piloted aerial systems (RPAS) that carry missiles or bombs – such as the iconic US-made MQ-1 Predator and MQ-9 Reaper – fully autonomous platforms are much less likely to be armed due to ethical concerns and technological limitations regarding targeting and with respect to rules of engagement. As a matter of fact, lethal autonomous weapon systems (LAWS) have been the object of a coalition of NGOs known as “Campaign to Stop Killer Robots.” Yet, there are drones capable of autonomously engaging targets such as Israel’s Harop (Harpy 2), a ‘kamikaze’ platform designed to detect and destroy enemy radars.

That said, drones are employed to carry out various types of missions. These include intelligence, surveillance, and reconnaissance (ISR); search & rescue (S&R); logistics; mine-sweeping and destruction of improvised explosive devices (IEDs); armed patrol; and even targeted killing. In such cases, drones operate on their own or in small numbers, and each is piloted by its own operator(s). However, advances in AI, robotics and data fusion may not only pave the way to fully autonomous systems capable of independently performing complex missions, but may also enable complex cooperation in a way that could radically change warfare.

THE ‘SWARMING’ CONCEPT

A paper by the US Air Force defines swarming as “a group of autonomous networked SUAS [small unmanned aircraft systems] operating collaboratively to achieve common objectives with an operator on or in the loop.”[9] Coordination and reactivity are of paramount importance, since they represent the key distinction between a real swarm and the employment of drones *en masse*. The latter occurs when a large number of drones is used against a single target, mostly in order to overwhelm it by saturating its defenses. Yet, each platform is controlled separately from others, and there is no datalink coordination between the drones themselves (even though the pilots can, of course, coordinate their action). On the contrary, drones operating in a swarm are all interlinked and in constant communication with each other. There is no clear threshold on the quantity of drones that must be connected to create a swarm, with figures ranging from a few hundreds to billions, also depending on their type and size. What is important is that they share information from their sensors and take AI-driven collective decisions toward the achievement of a single goal. This datalink and the AI software are therefore essential in creating the ‘hive mind’ that defines a swarm and allows it to effectively function; and each single drone forming a swarm is just a small component playing a specific role in a greater system which self-coordinates the actions of its elements in a dynamic manner. Certain drones would use their sensors to locate and track targets, sharing the information with the rest of the swarm; others would perform jamming and electronic warfare tasks; another category would engage hostile forces, etc. The swarm as a whole would react dynamically to changes in the battlespace by performing complex non-linear and counter-intuitive maneuvers.

It is therefore clear that swarming holds an immense potential, to the point that it may revolutionize warfare. Since they can patrol large areas with greater efficiency and shorter reaction times than human personnel, thus speeding up operations without risking the loss of lives, swarms would be particularly suited for search & destroy missions against enemy air defenses, submarines or mobile missile launchers; but also for ISR as well as counter-insurgency, over-the-horizon targeting, air combat, and anti-access / area denial (A2/AD). Symbiosis with manned platforms is also possible: For instance, F-35 fighters equipped with advanced data fusion software could control swarms and use them as force multiplies. Of course, creating a functioning and effective swarm requires top-tier technology in terms of both software and hardware; as it needs a powerful AI, advanced sensors, and powerful data links. Accordingly, swarms will probably take decades before being deployed and they will likely remain exclusive of high-tech militaries of developed countries.

Even though at present swarming remains largely theoretical and is still under development, major military powers like the US, China, Russia and others have shown a great interest in this concept and have already invested considerable resources in its development. For instance, in 2016 a US project successfully launched a swarm of 103

[9] https://www.af.mil/Portals/1/documents/isr/Small_UAS_Flight_Plan_2016_to_2036.pdf

Perdix drones from three F/A-18 Super Hornet fighters. Given the pace of technological advances over the past two decades, one can assume that swarming will only grow in importance in the near future, potentially altering the nature of warfare in the 21st century.

THE STRATEGIC IMPACT OF DRONE SWARMS

On the geopolitical level, it has been argued that swarms would continue the shift toward a 'more-than-human' geopolitics, where robotics and AI play a central role in the unfolding of events, and where the 'Baseworld' (the global net of military bases) constituting the framework of US power projection capabilities turns into a 'Roboworld' made of small lily pads scattered across the globe, which would virtually contract the spatial distances thus enabling the US to exert its power anywhere and almost constantly.[10] As far as the United States' near-peer competitors are concerned, experts believe that swarms may boost China's A2/AD capabilities and hamper freedom of navigation in the South China Sea; whereas for Russia, other than being A2/AD assets, they will also be extremely useful as force multipliers to compensate its manpower shortage through automation (which represents an important aspect of its military modernization, to the point that by 2025 it aims to have 30% of its entire military force composed of drones).[11] [12] In both cases, swarms may also empower them to quickly overcome weaker neighbors such as Taiwan or Ukraine, just to name two.

On the purely military plan, swarming could be the next step in the evolution of warfare, representing a real quantum leap when compared to traditional maneuver warfare.[13] The large-scale coordination between interconnected systems acting as a single and reactive entity would shorten the reaction times and compensate for individual vulnerability with the swarm's collective resiliency; thus significantly enhancing the warfighting capabilities of the armed forces deploying swarms and constituting a remarkable advantage over traditional militaries. This is the reason why major powers are interested in the concept and are seeking to gain an upper hand in the field.

However, this has raised fears of a new arms race centered on AI and automation that could have destabilizing consequences at the international level.[14] The reason is

---

[10] https://www.academia.edu/34424378/Robot_Wars_US_Empire_and_Geopolitics_in_the_Robotic_Age_Early_View_

[11] For more on Russia's military modernization, see: https://www.geopoliticalmonitor.com/russias-military-modernization-prevailing-in-limited-conflicts/

[12] https://www.academia.edu/38373946/Artificial_Intelligence_and_Future_Warfare_Implications_for_International_Security

[13] https://www.researchgate.net/publication/328508821_How_swarming_will_change_warfare

[14] https://www.academia.edu/41364115/Artificial_Intelligence_Drone_Swarming_and_Escalation_Risks_in_Future_Warfare

twofold. First, there are concerns that the possible over-effectiveness of swarms in search & destroy operations could undermine nuclear second-strike capabilities, which are largely based on mobile transporter erector-launchers (TELs) and on ballistic missile submarines. This would be particularly destabilizing for countries like China who have a rather small arsenal and whose retaliation force is centered upon a relatively small number of TELs and underwater vessels. Even though the real entity of this danger is debated and possibly overestimated, the perceived threat may be *per se* sufficient to destabilize the nuclear-based strategic equilibrium. Second, and partially linked with the previous point, the speed and efficiency of swarms compresses the reaction time for decision-makers to determine their course of action, thus prompting a 'use it or lose it' logic that would increase the likelihood of escalation, possibly to the nuclear stage. This problem, which becomes more acute in the case of a crisis, is also linked to other systems that have already been deployed (anti-satellite weapons) or that are being introduced (hypersonic missiles); and their potential combination may have mutually-reinforcing destabilizing effects whose consequences could be catastrophic.

LOOKING AHEAD

Even though it is at the early stages of development and experimental application, swarming is a concept that could radically change the nature of warfare in the coming decades. Given the technical complexity and the high costs of the necessary know-how, it is reasonable to assume that swarming will be the prerogative of major military powers, who would enjoy a significant advantage against both regular forces deprived of analogous capabilities and against insurgents thanks to the swarm's capacity to ensure a quasi-permanent and reactive monitoring over a large area.

Obviously, there are notable obstacles on the way: apart from legal and ethical issues, mastering the technology will take considerable time and investments; moreover, the swarm's effectiveness depends on the stable connection between its component and the proper functioning of the AI governing it, thus making it vulnerable to spoofing, jamming, cyber-attacks or simple technical malfunctioning. It is sure that as swarms are deployed and become more advanced, new efforts will be made to develop effective countermeasures. Considering the inherent decentralization of swarms and their ability to quickly react in a complex non-linear and counter-intuitive manner, it is likely that the best counter-swarm weapon will be another (larger and/or more advanced) swarm. What is certain is that drone swarms hold an enormous potential, and given the interest that major military powers are expressing toward this emerging technology, it is likely that drone swarms will eventually become a prominent feature of 21st century warfare.