Military Technology: The Realities of Imitation

According to a growing consensus, globalization and advances in communication are promoting the diffusion of defense-industrial capabilities, thus eroding the established position of Western countries. The empirical evidence, however, suggests that even with newly available opportunities, including cyber espionage, the most advanced weapon systems remain very difficult to copy and replicate.

By Andrea Gilli and Mauro Gilli

The maiden flight of the Soviet "Concordski" (Tupolev Tu-144) succeeded on 31 December 1968 – two months before the French Concorde. *Viktor Korotayev / Reuters*

Over the past 20 years, several observers, policy-makers, and scholars have warned of an impending transformation in world politics driven by globalization and the information and communication technologies (ICT) revolution. As a result of this transformation, it is alleged, countries lagging behind in military technology will be able to close the gap in military technology that separates them from the most advanced countries much more easily and quickly than they could in the past.

This view, implicitly or explicitly, underpins some of the most important foreign policy and defense issues of our times, such as the diffusion of defense-industrial capabilities around the world and its effects on international stability; the progressive erosion of the Western industrial leadership in the defense industry and what it means for conventional deterrence; the current and future military modernization of China and its implications for East Asia and world politics.

In this analysis, we explain why existing concerns exaggerate the ease with which countries lagging behind in the defense realm can catch up technologically with the industrial leaders. In the past, countries such as Imperial Germany, Imperial Japan, and the Soviet Union under Stalin managed to reduce the military-technological edge held by the most advanced states of their time by leapfrogging on foreign innovations through imitation, industrial espionage, or reverse engineering. However, military technology has become exponentially more complex in the meantime. As a result, imitating advanced weapon systems and replicating their performance has not become easier, as many believe, but has rather become more difficult. This does not mean that countries aiming at developing the most advanced weapon systems are preordained to fail. It means that to succeed, these countries need to undergo an extremely demanding, expensive, and lengthy process.

Conventional Wisdom on Imitation

According to the conventional wisdom, changes in the economics of production as well as in communication and production technologies allow countries lagging behind in military technology to skip the lengthiest and most expensive stages in the development of advanced weapon systems.

As a result, catching up technologically in the military realm should be allegedly easier and quicker than it used to be. Among the many changes purported to have brought about this change are the globalization of production and the resulting diffusion of industrial capabilities around the world; the advent of real-time communications and faster spread of knowledge and information; the increasing digitalization of data and the opportunity to steal it through cyber espionage; and the availability of software assistance for each stage of the production process, which could compensate for the lack of experience or capabilities on the part of the imitating countries – i.e., computer-assisted design (CAD), computer-assisted manufacturing (CAM), and additive manufacturing (3D printing).

Increasing Complexity

The mainstream view, that catching up technologically has become easier and will become even easier, seems to ignore a concomitant change in weapons production, namely the exponential increase in the complexity of military technology over the past century. This has made the imitation of the most advanced military platforms significantly more difficult – so much so as to countervail the facilitating effect of globalization and new communication and production technologies.

Weapon systems today encompass a much larger number of much more sophisticated components and subsystems than in the past. For example, the software for US jet fighters has increased from the 1,000 lines of code in the F-4 Phantom II (1958) to 1.7 million lines in the F-22 Raptor (2006) and 5.6 million lines in the F-35 Lightning II (2015). Even a very low defect rate, such as that reported for the US aerospace industry in 2000 (5.9 defects for every 1,000 lines of code), will lead to an extraordinarily large number of problems whose solutions might be mutually incompatible, and thus require additional (and hence extensive, expensive, and frustrating) effort. This is the reason why, nowadays, software has become the primary source of delay and cost overrun for major defense projects. Moreover, modern weapon systems are expected to operate under extremely demanding environmental and operational conditions. Jet fighters like the F-35 fly at supersonic speed, which entails very strict requirements in terms of materials employed and airframe design. Modern jet fighters like the F-35 face not only environmental challenges, but also operational ones: They are intended to operate in hostile airspaces where they will need to avoid detection, tracking, and engagement by enemy's integrated air defense systems or jet fighters. This poses as whole new set of problems, given advances in sensing technologies and signal processing. Consider that minor defects in the design or in the application of radar absorbing material are sufficient to compromise the low observability to radar of a "stealth" aircraft – for example, if a couple of screws are not perfectly aligned with the aircraft's airframe.

The Challenge of Imitation

As complexity increases, the number and depth of possible incompatibilities and vulnerabilities increase exponentially when developing a weapon system. Anticipating, detecting, identifying, understanding, and addressing all the possible incompatibilities and vulnerabilities entails extensive effort, experience, and time. Countries trying to copy a foreign weapon system will hence face a possibly infinite number of stumbling blocks: without the necessary industrial capabilities and experience, imitating countries might not even be able to detect, identify, or understand the problems they encounter.

China has struggled tremendously in imitating US 5th generation jet fighters.

First, attaining and maintaining the industrial, scientific, and technological capabilities required for copying advanced weapon systems has become extremely difficult. While in the early 20th century European countries could use their commercial industry to develop state-of-the-art weapon systems, this is no longer possible. Weapons development entails very specific problems that have no equivalent in the commercial sectors, such as safe storage of explosives activated by electronic circuits within a ship or an aircraft; or reducing the chance of detection to enemy sensors such as radar and sonar. For this reason, each platform under development requires specific dedicated equipment, laboratories, testing facilities, and specialized personnel – such as test ranges with radars operating at different frequencies and providing overlapping coverage; climatic laboratories and supersonic wind tunnels; test pilots with combat experience; or welders with submarine-specific experience. This degree of specialization means that the defense and civilian industries today differ markedly, so much so that even the defense and commercial divisions of companies like Boeing enjoy limited opportunities for synergies. Moreover, the fact that some components are dual-use does not mean that commercial companies will be able to integrate them successfully with thousands of other defense-only components; or that commercial companies will have the necessary expertise to ensure mutual compatibility among all the components, or the testing and production facilities required to detect and address vulnerabilities in the platform as a whole.

Second, the development of modern weapon systems takes many years and often decades, during which myriad problems may emerge. Even apparently minor ones, such as the oxidation of rubber seals, might pose a fatal threat to the platform being developed. The incompatibilities and vulnerabilities that emerge during weapons development are the inevitable product of integrating components that are not fully tested and developed; of developing weapon systems that operate under challenging and previously unexplored environmental conditions; and of having to deal with the counter-measures and counter-systems of more advanced enemies. The solutions to these problems are often found in less than straightforward ways, entailing extensive trial-and-error and the cooperation of multiple teams of designers, engineers, scientists, and specialized workers, each of whom bring their own expertise to the table. As a result, a part of the knowledge derived from this process is often tacit – it cannot be written down in terms of general rules and principles. This feature provides defense companies with an important advantage vis-à-vis would-be imitators.

Empirical Realities

The evidence from the defense industry does not support the conjecture that imitating modern weapon systems has become easier than it used to be, nor is there any indication to back up the claim that globalization and new technologies are facilitating technological catch-up. With regards to the alleged role of dual-use components, it is useful to consider the case of the Aegis anti-missile defense system, one of the most advanced military technologies of the U.S. Navy, which it fielded in 1983. The Aegis system relies on dual-use technology for more than 75 per cent of its components. Nevertheless, it remains unrivaled in

the world. Moreover, after France, Germany, Italy, and the UK had decided to develop a similar system in the 1990s, it took them two decades to field their Principal Anti Air Missile System (PAAMS), following repeated problems and failures. Similarly, access to foreign designs and blueprints is not sufficient to replicate an advanced weapon system. The Soviet Union experienced these challenges in the 1970s, when it managed to get its hands on the designs for the Anglo-French supersonic airliner Concorde. Because of the resemblance between the airframe of the Concorde and of the Soviet replica (the Tu-144), the latter was sarcastically nicknamed "Concordski" by Western journalists. However, beneath the surface, it was deficient in many realms, as the Soviet industry lacked the experience and industrial capabilities to understand the designs and replicate the processes, materials, and technologies used by Western European and North American companies.

There is little reason to believe that digital technologies have brought about or will bring about a revolutionary transformation, either. For instance, software assistance is no substitute for the experience, intuition, or understanding of designers, engineers, or specialized workers, but can only complement their skills. This was evident during the development of the F/A-18 Hornet. CAD failed to predict the F/A-18's aerodynamics problems, and provided little help in finding a solution – which was eventually found due to the experience of the engineers at McDonnell Douglas and extensive reliance on wind tunnels testing. Similarly, CAD is not a magic solution to engineering and industrial problems, as the UK learned during the development of its Astute-class nuclear-powered submarines. The British shipbuilding industry in fact had to modify its CAD software extensively before it could employ it to address the idiosyncratic requirements of submarines. Moreover, the employment of CAD required shipyard workers who could interpret and understand CAD outputs – which in turn takes extensive training and time.

We reach the same conclusion when looking at cases of defense cooperation, which generally give a less advanced country access to foreign designs and blueprints as well as to foreign know-how and experience. However, even in these instances, translating foreign information into a working weapon system has proved much more difficult than generally accepted. The case of Spain in the submarine sector is telling. After extensive cooperation in with France on submarine design and development, Spain decided to develop its own indigenous submarine. However, when the project had almost been completed, Spanish engineers discovered a design flaw in the new S-80 submarine: because of weight imbalance, it would not be able to resurface after submerging. This problem, which is currently being addressed, requires the lengthening of the hull. In additions to the cost and delay that this modification will entail, Spain will first need to expand its docking infrastructure, as the existing one is too small for implementing the required changes.

Finally, there is little reason to believe that the increasing digitalization of data will make the transfer of know-how easier. For example, standardized digital data did not ease or accelerate the transmission of complex design information among different companies participating to the Eurofighter Typhoon project, as the working practices of some of these companies were initially too different, which required that practices were standardized before the companies could take full advantage of digitalization. Along the same lines, additive manufacturing can be very effective for the production of parts for repair and maintenance, but cannot produce entire subsystems or modules (such as turbofan engines or radar systems). In turn, only specialized workers with extensive experience can carry out the replacements of defective or damaged parts in very advanced weapon systems.

Developing advanced weapons is a long, difficult, and expensive process.

China's Cyber Espionage Campaign

What about cyber espionage? Over the past few years, many have worried that cyber espionage might completely change the dynamics of industrial capitalism. Some have gone as far as to claim that it might bring about the greatest transfer of wealth in history. The case of China provides a particularly convenient test. China is one of the countries that has relied most extensively on cyber espionage: according to some accounts, it has stolen some 50 terabyte of data about the US stealth aircraft, as well as about key subsystems such as engines, radar, and missile navigation and tracking systems. Moreover, China has also relied extensively on traditional espionage, including the recruitment of spies who worked for the most advanced Western defense companies; the illicit purchase of proprietary data from foreign companies; and the purchase of foreign weapon systems from abroad with the goal of reverse-engineering them. China has also cooperated with countries such as Israel and Russia through joint-production programs with the goal of enhancing its industrial capabilities in aerospace; and it violated some licensing agreements with the goal of producing indigenous copies of foreign weapon systems. Last but not least, China is, without doubt, one of the countries that has benefited the most from globalization in recent decades, enjoying an unprecedented inflow of foreign direct investments. As a result, some of the most important companies in aerospace have opened subsidiaries or started joint ventures in China.

Nevertheless, China has struggled tremendously in imitating US fifth-generation jet fighters. The Chinese J-20 Black Eagle displays several features on the front, sides, and rear that would significantly increase the chance of detection to enemy radar (namely, canards in the front and unshielded engine nozzles in the back). China has also struggled with the development of reliable and powerful low-bypass turbofan engines that provide both enhanced maneuverability (thrust-vectoring) and sustained supersonic speed (supercruise). China has in fact encountered never-ending problems with the

Further Literature

Wedo Wang, **Reverse Engineering: Technology of Reinvention** (Boca Raton, FL: CRC, 2010).

Norman Friedman, **Naval Firepower: Battleship Guns and Gunnery in the Dreadnought Era** (Barnsley, UK: Seaforth, 2008).

Douglas Dalglleish / Larry Schweikart, **Trident** (Carbondale, IL: Southern Illinois University Press, 1984).

Christine Anderson / Merlin Dorfman (eds.), **Aerospace Software Engineering: A Collection of Concepts** (Washington, DC: American Institute of Aeronautics and Astronautics, 1991).

Obaid Younossi et al., **Military Jet Engine Acquisition: Technology Basics and Cost-Estimating Methodology** (Santa Monica, CA: RAND, 2002).

engine intended for the J-20 – including explosions during ground tests. In fact, the indigenous engines China has mounted on the J-20 have proven to be unreliable and underpowered – moreover, they do not provide either high maneuverability or sustained supersonic speed. Last but not least, there are serious doubts that China has been able to close the military-technological gap vis-à-vis the US in the electronics, given that China has apparently also encountered problems with the least demanding part of the onboard software, the flight-control software. There is then no reason to believe that China has had more success when it comes to the most demanding part of the onboard software, which carries out automatic detection of enemy aircraft at long range, exact geolocation, and high-confidence identification, as well as precise and continuous target tracking.

There is no substitute for the industrial capabilities and experience necessary to develop advanced military platforms.

Conclusions

With the rise of China and the resurgence of Russia, Great Power rivalry and military-technological competition are back at the center of international politics. Moreover, continued technological progress has given rise to potentially revolutionary technologies in the defense sector, such as unmanned and autonomous systems, cyber-capabilities, and quantum computing. Over the past few years, many have worried that globalization and new communication and production technologies might reshape the defense industry by promoting the diffusion of the capabilities, experience, and know-how from developed countries to less developed ones, in the process depriving the former of an advantage they have enjoyed at least since the Second World War.

In this analysis, we have argued that this view lacks empirical support. Globalization and new communications technologies permit the real-time transmission of unprecedented amounts of data. New information and production technologies allow for much more complicated computations and simultaneously permit a higher level of precision in manufacturing. None of them, however, provides a substitute for the industrial capabilities and experience necessary to develop advanced military platforms. The complexity of modern weapon systems gives rise to a never-ending number of incompatibilities and vulnerabilities. To anticipate, detect, identify, understand, and address all the possible incompatibilities and vulnerabilities, countries need equipment, laboratories, testing facilities, and specialized personnel as well as extensive experience with the system being developed and the environmental and operational context in which the system will be deployed. While countries might be able to learn from others' mistakes and experience, the development of advanced weapon systems will remain a long, difficult, and expensive process, especially in light of increasingly capable counter-systems and counter-measures.

Dr. Andrea Gilli is a Senior Researcher in Military Affairs at the NATO Defense College in Rome, Italy and an affiliate at CISAC, Stanford University. The views expressed in this article do not represent those of NATO or of the NATO Defense College.

Dr. Mauro Gilli is a Senior Researcher in Military Technology and International Security at the Center for Security Studies (CSS), ETH Zurich.

Some of the ideas presented in this brief are discussed more at length in their recent article "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage," in: *International Security* 43/3 (Winter 2018/19).

CSS Analyses is edited by the Center for Security Studies (CSS) at ETH Zurich. Each month, two analyses are published in German, French, and English. The CSS is a center of competence for Swiss and international security policy.

Editors: Christian Nünlist, Fabien Merz, Benno Zogg
Layout and graphics: Miriam Dahinden-Ganzoni
ISSN: 2296-0244; DOI: 10.3929/ethz-b-000323117

Feedback and comments: analysen@sipo.gess.ethz.ch
More issues and free online subscription:
www.css.ethz.ch/en/publications/css-analyses-in-security-policy

Most recent issues:

The OSCE's Military Pillar: The Swiss FSC Chairmanship No. 237
Long-distance Relationships: African Peacekeeping No. 236
Trusting Technology: Smart Protection for Smart Cities No. 235
The Transformation of European Armaments Policies No. 234
Trump's Middle East Policy No. 233
New Challenges in Nuclear Arms Control No. 232