THE GLOBAL RACE FOR TECHNOLOGICAL SUPERIORITY

Discover the Security Implications

edited by **Fabio Rugge**
introduction by **John R. Allen** and **Giampiero Massolo**

ISPI

BROOKINGS

THE GLOBAL RACE FOR TECHNOLOGICAL SUPERIORITY

edited by Fabio Rugge

BROOKINGS

Via Alamanni, 11 – 20141 Milano – Italy
www.ledizioni.it
info@ledizioni.it

The Global Race for Technological Superiority
Edited by Fabio Rugge
First edition: November 2019

This report is published with the support of the Italian Ministry of Foreign Affairs and International Cooperation (in accordance with Article 23- bis of the Decree of the President of the Italian Republic 18/1967), within the framework of the activities of the Centre on Cybersecurity jointly promoted by ISPI and Leonardo. The opinions expressed are those of the authors.

Print ISBN 9788855261432
ePub ISBN 9788855261449
Pdf ISBN 9788855261456
DOI 10.14672/55261432

ISPI. Via Clerici, 5
20121, Milan
www.ispionline.it

Catalogue and reprints information: www.ledizioni.it

BROOKINGS

The Brookings Institution is a nonprofit organization devoted to independent research and policy solutions. Its mission is to conduct high-quality, independent research and, based on that research, to provide innovative, practical recommendations for policymakers and the public.

Table of Contents

Introduction

In 1983, the Russian-born naturalised American writer Isaac Asimov was invited to imagine what 2019 would look like[1]. The idea was to reprise what George Orwell did with *1984*. Among his predictions, Asimov was certainly right about *computerisation* – what he called "*the march of computers*"; speaking of which he added "*After industrialisation, the shift from the farm to the factory was rapid and painful. With computerisation the new shift from the factory to something new will be still more rapid and in consequence, still more painful*". It was a harsh premonition. Indeed, great innovations in the field of Artificial Intelligence (AI), quantum computing, robotics, space technologies, cognitive science and biotechnologies – just to name a few – and their introduction into our lives have an impact not only at the economic, sociological, cultural and cognitive levels, but also in geopolitical terms. Technology is a key driver of any transformation of power at the international level. And as such, we are witnessing increasing concerns over new global competition, fostered by innovative digital technologies, which could abruptly change balances of power in the international system. The reason is straightforward: the first to exploit the potential of these ground-breaking innovations will be the first to acquire a strategic advantage. In brief, technology will be one of the enablers of sovereignty in all five domains (air, land, sea, space, and cyberspace).

[1] I. Asimov, "Asimov's New World", *The Toronto Star*, 31 December 1983.

Cyberspace and digital technologies have become far too relevant for everyday life not to also be the lynchpins around which national interests naturally collide. Every state operates in an increasingly contested cyber domain and is actively engaged in advancing its relative cyber power and tech superiority. Artificial Intelligence, quantum technologies, robotics, autonomous weapons, and neural implants will all concur in transforming future warfare in ways we are only starting to understand. Quantum technologies, for instance, will make the most advanced encryption techniques obsolete while enabling the development of "non-hackable" information and communication technology (ICT) systems.

In this new race for technological leadership, the borders between the civil and military spheres are blurred. Both private and public actors are engaged in developing and adopting these technologies. In some countries, innovation largely comes from the private sector and academia, and thus, there is a renewed urgency to ascertain how states can best leverage and financially sustain these new technologies while also protecting them from hostile takeovers, mitigating brain drain of the human capital essential to lead the race, and decoupling the IT supply chain from the risks embedded in new ICT products, as in the case of 5G technologies.

This Report by the ISPI Center on Cybersecurity and the Brookings Institution analyses how the race for technological superiority is reshaping the international arena, and how technological superiority has become a strategic enabler of sovereign power in the XXI century. It addresses some of the following questions: who are the key leaders in this quest for tech superiority? What is the impact of disruptive technologies in military and security affairs? What role do states play in harvesting and protecting research in disruptive technologies?

We are on the cusp of one of the greatest technological revolutions since the invention of the printing press, and there is still significant debate at the political and academic level about the true impact of such innovations. Nevertheless, it is possible

to identify many of the primary threats coming from ongoing technological progress. As the editor of the report, Fabio Rugge argues that for analytical purposes, it is possible to group the challenges to the international order into two distinct – but, in reality, overlapping – categories. The first concerns the disruptive military applications of these technologies, which could result in a strategic advantage for some. For example, this is the case of hypersonic weapons, which are apparently invulnerable to any anti-missile systems, or the application of AI to cyber offensive operations. The second category refers to the challenges that technological innovations pose to policy-makers and military commanders when they are called to operate. This includes ambiguity (in terms of attribution and recognition), entanglement (concerning the interconnectedness of civil and military systems – including nuclear ones), and surprise (with regard to the unpredictability of the strategic environment). Therefore, the risk is that technological development could produce a thicker "fog of war", which may eventually prevent anyone from winning.

The security implications are enormous and call for an extensive revolution in military affairs. As Gabriele Rizzo explains, if the West wants to keep its military edge in the future, it should be able to adapt to the evolution brought about by the second "Machine Age", which is driven by three main forces: complexity, convergence and exponentiality. It is still too early to fully understand the effects of this technological revolution on military affairs. However we can already foresee how it will change warfare in the coming decades: hyperwar, the AI-fueled, machine-waged conflict[2], is looming, and thus, militaries should be prepared for "instant decision, perfect action". The United States is already integrating radical technologies within its armed forces, a key step for maintaining its military edge. Nevertheless, this process is neither straightforward nor easy, especially if we consider that most of this technological potential is still to be unveiled.

[2] J.R. Allen and A. Husain, *On Hyperwar*, US Naval Institute, vol. 143, no. 7, July 2017.

In some cases, the disruptive impact of innovative discoveries is already tangible, especially on network and communication systems and technologies. This is the case with 5G, for example. The quest to secure what Tom Wheeler and David Simpson call, "the most important networks of the XXI century" is fundamental to the future prosperity of our nations. However, as argued by the authors, in the ongoing political debate about 5G there is a hyper focus on China and its companies such as Huawei and ZTE, which could lead to misinterpreting the important aspects of having a safe 5G. Because of the intrinsic characteristics of 5G networks, we must focus on new approaches to cybersecurity. Therefore, the authors call for new efforts to be made both at a private (companies must be held responsible for a new cyber duty of care) and government level (with a new cyber regulatory paradigm), which will allow the United States (and those who are willing to follow it) to win the real 5G race.

Moreover, the application of AI algorithms on a traditional and often forgotten type of warfare – electronic warfare – could generate dramatic consequences for the targeted actors. As Tom Stefanik explains in his chapter, ongoing research efforts, especially in the United States and China (and Russia) attempt to apply particular types of algorithms to functions within the overall electronic warfare signal process chain. Although there have not yet been concrete applications, the possible outcome could be disastrous. With ongoing developments in the field of autonomous weapons or that of remote control of defence/offence systems, which rely on an effective electromagnetic environment, the possibility of interference could potentially alter human control over new technologies, including weapons.

The security implications of technological developments also pertain to securing the "hearts and minds" of individuals. So far, as John Villasenor argues, most of the literature and public debate has focused on how Artificial Intelligence can be used in misinformation campaigns, while overlooking its contribution to detecting and countering such events. For example, AI

could be adopted to identify deep-fake episodes, or to block AI-enabled bots, which are crucial to spread misinformation through social networks. This could be crucial on some occasions, as in the run up to an election or referendum, when risks of disinformation and fake news are at their highest.

Cyberspace is thus a crucial, contested domain for achieving technological superiority. In light of this, it is imperative that states elaborate new strategies and regulations in order to avoid dangerous escalations and, at the same time, properly secure their societies. According to Mariarosaria Taddeo, current strategies and norms are inadequate to address these challenges. Indeed, in cyberspace, threats are asymmetric and attacking is cheaper and easier than defending. Therefore, conventional deterrence is problematic and entails a high-risk of escalations. In her chapter she calls for a re-conceptualisation of cyber-deterrence, which should shift from threatening to prevailing, and of norms of state behaviours, which should complement deterrence.

However, so far finding international agreement on digital affairs has proven very difficult. One of the reasons lies in the different approaches that liberal democracies and authoritarian regimes have to technology. The latter are at the forefront in applying and using new technologies to support their strategic aims both domestically and internationally, where they are promoting an agenda that is in contrast with the founding principles of cyberspace. However, Samuele Dominioni argues that because of inner institutional weaknesses (both economic and political), in the long run authoritarian regimes will not be able to lead the race for technological superiority unless they reform their governance in a pluralistic sense.

Overall, it is possible to claim that the current race to technological superiority is a catch-all race, an event that happens very seldom in history. This Report by ISPI and the Brookings Institution is an effort to better understand the comprehensive transformation we are now facing and how it will change the way we experience the world. We may not have the same

admirable precognitive capabilities Asimov had, but we are fully committed to making *computerisation* less painful and disruptive than he had predicted. To this end, it is essential that states make efforts at the international level to find shared and compatible approaches that will regulate competition and enhance trust.

John R. Allen
President Brookings Institution

Giampiero Massolo
President ISPI