BRUSSELS SCHOOL OF GOVERNANCE
CENTRE FOR SECURITY, DIPLOMACY AND STRATEGY

CSDS POLICY BRIEF • 3/2021

High Tech, Low Take? The Strategic Impact of Disruptive Technologies

By Antonio Missiroli | 1 April 2021

Key Issues

- The development and use of digital technologies are fundamentally different from the past as they stem primarily from the private commercial sector, are easily accessible and poorly regulated at international level. They can be 'weaponised'.
- The spread and use of digital technologies have created new spaces and opportunities for hostile activity and are changing the global balance of power, not only between states but also inside and across them. The West risks losing the technological edge it has enjoyed for decades to the benefit of illiberal forces and splitting internally between 'haves' and 'have-nots'.
- While efforts are now underway in both NATO and the EU to tackle those risks collectively, challenges remain.

At both national and international levels, new and potentially disruptive technologies are dramatically changing the way deterrence, defence, and, more broadly, security policies are conceived and carried out.

Technology has deeply influenced – and sometimes contributed to revolutionising – warfare, from the Stone Age to Hiroshima. Warfare, in turn, has often boosted technologies later applied to civilian life. Purposeful human manipulation of the material world has virtually always been dual-use – from hunting tools to boats, from explosives to combustion engines, from railroads to satellites – as have platforms like chariots, galleys, mechanised vehicles, and aircraft. Science-based engineering has often supported warfare, including fortifications, artillery, communications, surveillance, although systematic state-funded research and development (R&D) for military purposes started only during the Second World War (and, arguably, peaked during the Cold War).

Technology harnessed by skilled commanders has always acted as a force multiplier in war, allowing them to inflict more harm on the enemy or limit harm on their own side. Throughout history, technological superiority has generally favoured victory, but never guaranteed it: comparable adversaries have often managed to match and counter technology-driven tactical advantages (even within the same conflict), while manifestly inferior adversaries have frequently (and sometimes successfully) adopted 'asymmetric' tactics in response. In other words, the value of technology in warfare is always relative to the adversary's capabilities and responses.

This time it's different

Yet what we are experiencing now, at least since the 1990s, is exponential technological progress that is affecting all realms of life – not only, or even primarily, the military. In the deterrence and defence realm, the development and application of information communications and technology, resulting in precision-guided weapons and so-called 'net-centric' warfare, was initially conceptualised as another 'revolution in military affairs' (previous ones include the advent of the chariot in antiquity, gunpowder at the dawn of the modern era, mechanised units after the Industrial Revolution, and nuclear weapons since the Second World War). In retrospect, net-centric warfare now appears more like an evolutionary and incremental process of transformation than a revolution in its own right; yet the loss of control and lack of predictability engendered by the new technologies have serious implications for deterrence, defence, and security at large. Just like previous (r)evolutions, the current one is expected to alter dramatically the global balance of power, and not only between empires, city-states, or nation-states, as in the past, but also within and across actors – as, for instance, big tech companies begin to cultivate the level of power (and even status) often associated with statehood.

This acceleration of technological development has been driven by the private commercial sector, especially in the digital domain, and has created an increasingly dense network of almost real-time connectivity in all areas of social activity that is unprecedented in scale and speed. As a result, new technologies that are readily available – cleverly employed and combined – offer both state and non-state actors a large spectrum of new tools to inflict damage and disruption above and beyond what was imaginable a few decades ago, in warfare as well as peacetime. Targeted are not only traditional military forces on the battlefield but also civilian populations and critical infrastructure.

Moreover, most of these technologies (with the possible exception of stealth and hypersonic weapons) emanate from a public policy ecosystem fundamentally different from that of the traditional defence-industrial model, which was based on top-down long-term capability planning and development, oligopolistic supply (a small number of sellers with no real price competition), and monopsonic demand (a single buyer). Military R&D then resulted in technology – such as radars, jet engines, or nuclear power – that was later adapted and commercialised for civilian use. Now these new technologies are being developed from the bottom up and with an extremely short time from development to market: only after hitting millions of consumers worldwide and creating network effects do they become dual-use – and thus also 'weaponisable'.

In other words, the vector of dual-use innovation has significantly shifted in most sectors, with spillover and spin-off effects stemming primarily from the *civil* realm. Investment in science and technology (S&T) is now mainly driven by market considerations, and the scale of its expenditure dwarfs defence-specific S&T spending. This gives rise to technology areas where defence relies completely on civil and market developments. The new superpowers are the private big tech consumer giants from the West Coast of the United States and mainland China.

New contested spaces, new weapons

The latest technological breakthroughs have fostered, in particular, the development and 'democratisation' of so-called 'standoff' weapons: these are armed devices which may be launched at a distance sufficient to allow attacking personnel to evade defensive fire from the target. As a result, they are challenging the underlying trade-offs between delegation and control and generating new ethical and legal dilemmas by making it possible to operate unmanned platforms from a distance – first for reconnaissance and surveillance, then for punishment and decapitation missions. These new weapons are also providing an incomparable degree of discretion (low visibility, also domestically) and deniability (also internationally). Most importantly, some are now easily accessible on commercial markets and relatively simple to operate, further breaking the traditional monopoly of states over weaponry and the legitimate use of force and thereby opening up new spaces for different types of warfare.

Cyberspace-based weapons go even further – when used for sabotage (cyberattacks) and subversion

(disinformation and destabilisation) rather than just espionage – in coercing and disrupting while preserving discretion and deniability, as they operate in a purely man-made and still poorly regulated environment that relies entirely on technology to work. Digital weapons can indeed achieve strategic effects comparable to warfare without resorting to *direct* physical violence. As opposed to nuclear weapons, cyber weapons are not for deterrence but for actual and constant use, and can be operated by states as well as proxies and private organisations without geographic or jurisdictional constraints: attribution is slow and difficult, and retribution is risky.

The media space has become an additional battlefield as a transnational global public sphere where perceptions of right and wrong, victory and defeat, are shaped and consolidated at lightning speed. Social media have not been militarised but have certainly been weaponised, not only by state or state-sponsored actors but sometimes also by individual citizens/consumers acting as more or less unwitting auxiliaries. And while cyber-enabled sabotage requires high levels of know-how but relatively little manpower, cyber-enabled subversion is much simpler to design but requires a critical mass of users to spread narratives.

Outer space has so far remained relatively immune from these trends, in part thanks to the provisions of the 1967 Outer Space Treaty, and in part due to the risks intrinsically associated with the possible use of force (e.g. debris). Technological developments *up there* have been focused on facilitating activity *down here* (mainly satellite communications for broadcasting and navigation) for both public and now increasingly also private actors, with all the resulting democratisation effects. The most capable states have indeed militarised space (i.a. with the creation of Space Commands) but, although ever more countries are entering the game, a Star-Wars-like weaponisation of outer space still seems an unlikely scenario.

Last but not least, artificial intelligence, machine learning, big data, and autonomy – as interrelated, mutually reinforcing general-purpose technologies – are opening up just another space in which international law is nearly silent and some concepts and their interpretations are contested, as shown by the ongoing discussions on Lethal Autonomous Weapons Systems (LAWS) at the UN and beyond. Their disruptive potential is huge, also in strictly military terms, and so is the risk of an unrestrained arms race, especially in the current geostrategic and diplomatic environment – and also in the absence of a transnational 'epistemic community' of experts pushing (as in the past with weapons of mass destruction) for arms-control-type arrangements, restrictive international regimes, or binding codes of conduct. It is true that global conventions governing new technologies tend to be crafted only after those technologies have been used for some time, thus reaching a certain degree of maturity and raising awareness of the need to regulate them. In this case, however, traditional approaches to disarmament and non-proliferation would probably be problematic to enforce as digital platforms would be difficult to detect, inspect, verify, certify, and dispose of.

“Traditional approaches to disarmament and non-proliferation would probably be problematic to enforce as digital platforms would be difficult to detect, inspect, verify, certify, and dispose of.”

On the other hand, these new technologies could also prove transformational rather than just disruptive: they could in fact be used more constructively, e.g.

for fact-checking and trend analysis, prediction and simulation (as in life sciences), or logistics and equipment maintenance purposes (as in business), thereby facilitating rather than complicating decision-making. Technology can be both a boon and a bane.

Decline of the West?

In this context, two closely related risks weigh on the West as a whole. The first is a potential loss of the collective technological superiority it has enjoyed over the past 50 years (and especially after the Cold War). China is already a peer competitor in most dual-use technologies and benefits from a tested model of public-private partnerships, e.g. on big data and facial recognition; Russia excels in some military-related ones and relies on a tight command-and-control system; and new actors with deep pockets and/or high ambitions are emerging in critical areas. Weaponisation of intent and democratisation of access could indeed alter the strategic balance of power, potentially in favour of illiberal forces.

The second risk is a growing transatlantic gap and disconnect between the 'haves' (the US as a system) and the 'have-nots' or 'have-littles' (Europe). Even if the relations between the tech giants from the West Coast and the federal authorities in the East are often bumpy, the US retains a critical mass of know-how and a dynamic ecosystem where innovation can be 'nudged' and competition (even if oligopolistic) creates global winners. Europe has its own poles of scientific excellence and industrial expertise, an open economy, and a decent record of pooling assets, but it struggles to harness all that to comparable levels: as *The Economist* recently pointed out, the only major European-made global platform is … Spotify.

The diminishing public resources generally devoted to R&D and S&T, especially if measured against the scale of investment required and the financial risk inherently linked with ground-breaking research, render even the recent efforts made by some major European governments – however innovative – largely insufficient to address that gap. This shortfall, along with the prospect of normative divergence across the Atlantic (e.g. on data protection or corporate taxation), may well have a serious impact on the West's political solidarity and interoperability across the board.

Lately, while the G-7 has provided a forum to articulate shared principles and guidelines, NATO and the EU have come to the realisation that these risks may need to be addressed collectively. A couple of years ago NATO set up a high-level Innovation Board that brings together all the relevant stakeholders – including Supreme Allied Command Transformation in Norfolk and the Science and Technology Organisation in Paris – and is tasked with achieving a better common understanding of the implications of these emerging and disruptive technologies (EDT) and proposing a fresh strategy for the Alliance to adapt and, possibly, adopt them. For its part, the EU has set up a dedicated Directorate-General for Defence Industry and Space in the Commission and launched a number of relevant projects in the framework of Permanent Structured Cooperation (PeSCo) and the new defence-related funding schemes (European Defence Fund and European Defence Industrial Development Programme) agreed since 2017.

Challenges and opportunities for collective action

All this is encouraging but, of course, many challenges still lie ahead. First, inside NATO, there still is no clear agreement on what to do collectively in this domain – also in terms of funding, procurement, and acquisition of potential new assets. These processes normally take a long time even when agreement already exists, and the asymmetry in capabilities among the 30 Allies does not facilitate a shared approach. Moreover, due to the nature of these new technologies, even tailor-made schemes like those adopted decades ago for the Airborne Warning And Control System (AWACS) fleet would probably not do the trick, as it has now become essential to involve the private sector and cater to venture capital.

As for the EU, where the case for pooling and sharing is clearer, the problem lies primarily in the scarcity of both national and EU-owned resources allocated to the effort and the proliferation of micro-projects presented for funding so far. This could

lead to fragmentation and waste while also failing to create the necessary synergies between civilian and military-related research as well as between national and EU levels – not to mention the need to draw in private companies and investors.

For both NATO and the EU, at any rate, selecting a few clear priorities, allocating adequate resources, and setting appropriate incentives for public-private partnerships could turn those challenges into consequential opportunities. All these issues will also have to find the place they deserve in the forthcoming strategic reflections planned by the two organisations, namely NATO 2030, due to feed the June summit of the Alliance and, possibly, a review of the 2010 Strategic Concept; and the Union's 2022 Strategic Compass, expected to update the 2016 Global Strategy.

Policy innovation can also help build on the two organisations' respective strengths (standardisation and interoperability for NATO, regulation and policies of scale for the EU), leverage the combined assets and capabilities of their members, and avoid unnecessary duplication and competition. The recovery plans post-COVID may also help skilled labour from the hard-hit civilian aerospace sector shift to the defence industrial and technological base. Finally, policy implementation matters too: for instance, the Defence Pledge adopted by NATO members at their Wales Summit in 2014 set a target not only for national defence spending (2% of GDP by 2024) but also for expenditure on major new equipment, including R&D (20% of total defence spending). It would certainly be beneficial for all – in particular the EU members of the Alliance, who have also signed off to their own Capability Development Plan – if this second commitment received at least equal political attention.

ABOUT THE AUTHOR

Antonio Missiroli

is an Adjunct Professor at the Brussels School of Governance. He served as NATO Assistant-Secretary General for Emerging Security Challenges from December 2017 to November 2020. Prior to joining NATO, Dr. Missiroli was the Director of the European Union Institute for Security Studies (EUISS) in Paris (2012-17). Previously, he worked at the Bureau of European Policy Advisers (BEPA) of the European Commission (2010-2012); as Director of Studies at the European Policy Centre in Brussels (2005-2010); and as Senior Research Fellow at the W/EU Institute for Security Studies in Paris (1998-2005). He was also a Visiting Fellow at St Antony's College, Oxford (1996-97).

He has also taught i.a. at SAIS/Johns Hopkins (Bologna), the College of Europe (Bruges) and Sciences Po (Paris). Dr. Missiroli holds a PhD in Contemporary History from the Scuola Normale Superiore (Pisa) and a Master's degree in International Public Policy from SAIS/Johns Hopkins.

antonio.missiroli@gmail.com

The **Centre for Security, Diplomacy and Strategy (CSDS)** seeks to contribute to a better understanding of the key contemporary security and diplomatic challenges of the 21st century – and their impact on Europe – while reaching out to the policy community that will ultimately need to handle such challenges. Our expertise in security studies will seek to establish comprehensive theoretical and policy coverage of strategic competition and its impact on Europe, whilst paying particular attention to the Transatlantic relationship and the wider Indo-Pacific region. Diplomacy as a field of study will be treated broadly and comparatively to encompass traditional statecraft and foreign policy analysis, as well as public, economic and cultural diplomacy.

The **CSDS Policy Brief** offers an interdisciplinary platform for critical analysis, information and interaction. In providing concise and to the point information, it serves as a reference point for policy makers in discussing geo-political, geo-economic and security issues of relevance for Europe. Subscribe here. If you consider contributing, contact the editor Prof. Michael Reiterer: michael.reiterer@vub.be

Follow us at:
Twitter @CSDS_Brussels LinkedIn CSDS Brussels Youtube CSDS
http://csds.brussels-school.be

BRUSSELS SCHOOL OF GOVERNANCE

The Brussels School of Governance is an alliance between the Institute for European Studies (Vrije Universiteit Brussel) and Vesalius College.

Visitor's address:
Pleinlaan 5, 1050 Brussels, Belgium
Mailing address:
Pleinlaan 2, 1050 Brussels, Belgium

info_bsog@vub.be

www.brussels-school.be