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

ISPI 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

1. Emerging Disruptive Technologies and International Stability

Fabio Rugge

Tutto si muove, tutto corre, tutto volge rapido.
Umberto Boccioni

Science gathers knowledge faster
than society gathers wisdom.
Isaac Asimov

Back to the Futurists

At the turn of the XX century, in the city where ISPI was established, velocity became a cult. It was an era marked by extraordinary technological progress, and the Futurist Movement, in its 1909 Manifesto, proclaimed that the speed of change in technology should inform – and, in fact, define – both cultural and political progress, in addition to the idea of beauty. The "old world" seemed, in fact, to be rapidly drifting away, as new inventions (electricity, railways, telegraph, cars, planes, …) were delivering a whole new range of possibilities, waiting to be explored. It was also an age of profound change affecting domestic societies and political life, along with international relations, in the wake of two world wars. While financial integration was rampant, the globalization process also saw increasingly frequent trade wars and growing unemployment, poverty and social unrest, spurring great migrations (within Europe, and from Europe, to the rest of the world). As European leaders engaged in negotiating many international "great treaties" (many of which had no follow-up whatsoever), faith in international solidarism was slowly fading away, as international cooperation and multilateralism were increasingly perceived as inadequate to solve international issues. Parliaments were

seen as incapable of delivering timely results, thus providing fertile ground for the rise of nationalism throughout Europe, and for the idea that sovereignty should not have any political, legal or even moral restraints. Deep ideological differences were beginning to emerge in the international community, causing unsolvable cleavages between States that were actively engaged in an industrious rearmament, driven by the application of new technologies and aimed at providing a whole new set of warfare capabilities. At the domestic level, too, "strong men" were beginning to dominate the political scene exploiting the new possibilities provided by the modern media and forging new and more direct connections with the national masses, whose *vox populi* was getting increasingly louder. There was, in sum, a growing sense of frustration with political structures perceived to be increasingly unable to cope with the ongoing technological and social innovations. The Futurists pointed this out while giving voice to the idea that politics should instead be fast, powerful, dynamic and revolutionary at least as much as the innovations brought about by technology and already underway in society. Ironically, the Great War, which erupted only a few years after the publication of the Futurists' Manifesto, was the very opposite of velocity: it was a trench war.

In many ways, the quest for military innovation is the age-old competition between the sword and the shield, but the current debate around disruptive technologies – which is occurring in a not too different cultural and political setting than that of the beginning of the century, and seems to eco its hype – has taken a new attention. The issue is largely perceived and faced with a sense of urgency since, for the first time in centuries, the West appears to be losing the technological initiative that has historically been associated with its hegemony on the international system[1]. This power transition, in turn, is nurturing

[1] "Aggressively pursuing technological innovation and introducing those advances into the force promptly will be critical to overcoming operational challenges and positioning the U.S. military for success. We applaud the National Defence Strategy for emphasizing this issue. We remain concerned, however,

concerns about the West's ability to prevail in a future military confrontation[2], and it is also (as was the case with the Futurist Movement!) giving rise to an existential dilemma of sorts: are liberal democracies better suited, or even able, to deliver on this crucial account? The distance from the reassuring moral superiority self-proclaimed by the West during the Cold War is striking. When Ronald Reagan launched his "Strategic Defence Initiative" for developing a comprehensive strategic ballistic missile defensive system in 1983, he was confident that, in years to come, the US would have "naturally" retained technological dominance over the Soviet "Empire of Evil", and that

---

that America's edge is diminishing or has disappeared in many key technologies that underpin U.S. military superiority, and that current efforts to offset that decline are insufficient", Providing for the Common Defence, The Assessment and Recommendations of the National Defense Strategy Commission, November 2018. See also: John R. Allen, "The Next Space Race Is Artificial Intelligence. And the United States is losing Foreign Policy", 3 November 2017.

[2] "During the next decade, the rise of new powers and the accelerating diffusion of advanced technology throughout the international system will pose significant challenges to U.S. technological dominance in military affairs. […] In recent years, however, the notion of such dominance has been more akin to a presumption than a reality. […] America's technological dominance is far more fragile than is commonly understood", S. Brimley, B. FitzGerald, and K. Sayler (Foreword by P.W. Singer), *Game Changers. Disruptive Technology and U.S. Defense Strategy*, Center for a New American Century, September 2013, p. 7 and 9. See also: "Yet if ever there were a time to get serious about the coming revolution in military affairs, it is now. There is an emerging consensus that the United States' top defense-planning priority should be contending with great powers with advanced militaries, primarily China, and that new technologies, once intriguing but speculative, are now both real and essential to future military advantage. Senior military leaders and defense experts are also starting to agree, albeit belatedly, that when it comes to these threats, the United States is falling dangerously behind", C. Brose, "The New Revolution in Military Affairs. War's Sci-Fi Future", *Foreign Affairs,* May/June 2019, p. 123. See also: "However, the U.S. military must prepare for a future in which the United States may no longer possess technological predominance, particularly through focusing on the human factors and organizational capacity that are critical determinants of successful defense innovation", E.B. Kania, *Battlefield Singularity. Artificial Intelligence, Military Revolution, and China's Future Military Power*, Center for New American Security, 28 November 2017a.

this superiority would have ultimately ensured victory[3] – 1989 seemed, at the time, to confirm that axiom. Western democracies, instead, now see themselves confronted with competitors that ostensibly reject the model of liberal democracy (more precisely, they declare it moribund), while greatly succeeding in developing cutting-edge technology of strategic relevance, leveraging their greater control on the private sector and their longer-term planning capability.

So, the question arises: how well-grounded is today's widespread anxiety over the possibility that disruptive technologies may, in a not too distant future, significantly destabilize the international security environment? Disruptive technologies will indeed have an impact on the international order, affecting both the international Balance of Power and the "rules of the game", but it is difficult to point to just how, as it may well be that we are caught in Amara's law, by which we overestimate the effect of a new technology in the short term, while failing to correctly appreciate its impact in the long run. Is anxiety the right response to the uncertain future that awaits us?

[3] "Let me share with you a vision of the future which offers hope. It is that we embark on a program to counter the awesome Soviet missile threat with measures that are defensive. Let us turn to the very strengths in technology that spawned our great industrial base and that have given us the quality of life we enjoy today. […] I know this is a formidable, technical task, one that may not be accomplished before the end of this century. Yet, current technology has attained a level of sophistication where it's reasonable for us to begin this effort. It will take years, probably decades of effort on many fronts. There will be failures and setbacks, just as there will be successes and breakthroughs. And as we proceed, we must remain constant in preserving the nuclear deterrent and maintaining a solid capability for flexible response. But isn't it worth every investment necessary to free the world from the threat of nuclear war? We know it is", Ronald Reagan's Address to the Nation, 23 March 1983.

Future Disruptive Technologies, the Cyber Domain and International Stability

Throughout history, we have seen how technological innovation proceeds faster than our understanding of its potential applications and of its military-strategic implications – the advent of computing power and new technologies greatly increased this gap[4]. Our "increasingly complex security environment is defined by rapid technological change"[5] and technological superiority has become one of the defining paradigm of the current competition between states. Technological dominance, however, does not mean *per se* military superiority, as technological innovation needs to be weaponized and requires policies, concepts and doctrines of use for effective exploitation[6].

[4] "If Moore's Law holds true the way it has for the past 40 years, […] in the strategic horizon of the next 25 years, we will see technologies literally one billion times more powerful than today". S. Brimley, B. FitzGerald, and K. Sayler (2013). See also: "Advances in the world of digital interconnectedness have many of the attributes of the quintessential disruptive technology that gunpowder exemplifies, with the fundamental difference that the changes brought about by the omnipresence of cyber technologies are happening at an exponential pace", S. Ülgen, *Governing Cyberspace. A Road Map for Transatlantic Leadership*, Carnegie Endowment for International Peace, 2016.

[5] United States of America, *National Defence Strategy*, 2018, p. 3.

[6] "Technological surprise is in many cases, not necessarily entirely based on new technology arriving on the battlefield but rather the use a technology coupled with new tactics that causes the surprise", G.H. Heilmeier, "Guarding Against Technological Surprise", *Air University Review*, September-October 1976. See also: "Does cyberpower, particularly military cyberpower, matter? […] If control, influence, or competence in the medium has little to do with the delivery of military power in the more conventional realms, then no one would need it, except perhaps for bragging rights", M.C. Libicki, "Military Cyberpower", in F.D. Kramer, S.H. Starr, and L.K. Wentz (eds.), *Cyberpower and National Security*, National Defense University Press, April 2009. See also: "Evolve innovative operational concepts. Modernization is not defined solely by hardware; it requires change in the ways we organize and employ forces. We must anticipate the implications of new technologies on the battlefield, rigorously define the military problems anticipated in future conflict, and foster a culture of experimentation and calculated risk-taking. We must anticipate how competitors and adversaries

Conversely, military innovation does not necessarily require new technologies, as military advantage may also result from the innovative use of existing technologies[7]. Moreover, long-term shifts in the Balance of Power may be indirect, as an effect of the economic power brought about by technological innovation. In any case, a strong political drive is another crucial condition to develop and introduce new military technologies, because of the resistance to be sidestepped on the part of what Senator John McCain once called "the military-industrial-congressional complex", "whose entire livelihood depends on developing, producing, acquiring, operating, and maintaining traditional defense systems in traditional ways"[8].

---

will employ new operational concepts and technologies to attempt to defeat us, while developing operational concepts to sharpen our competitive advantages and enhance our lethality", *National Defence Strategy*…, cit., p. 7. See also: "Yet the relative impact of technological change often depends as much or more on how people, organizations, and societies adopt and utilize technologies as it does on the raw characteristics of the technology" […] "Decades of research demonstrates that the impact of technological change on global politics – whether it is change in economics, society at large, diplomacy, or military power – depends much more on how governments and organizations make choices about the adoption and use of new capabilities than on the technologies themselves. Scholarship on military innovation by Barry Posen, Stephen P. Rosen, and others shows that technological innovation alone rarely shapes the balance of power. Instead, it is *how* militaries use a technology that makes a difference", M.C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power", *Texas National Security Review*, vol. 1, no. 3, May 2018, p. 38 and 43.

[7] In an internal memo of October 1984, for instance, the CIA, when confronted with the problem of defining "technological surprise", wrote: "Two types of technological surprise can be addressed: the sudden advance in applied science of technology which for some period provide the adversary with some sort of economic or military advantage; and the application of some known technology in an unusual or innovative manner", https://www.cia.gov/library/readingroom/docs/CIA-RDP91B00046R000300390029-6.pdf

[8] C. Brose (2019), p. 133. See also: "History suggests that DOD – and in particular, the military services – will resist investment in technologies that call into question preferred legacy platforms, core competencies and concepts of operations. [T]oday's innovators will need to compete against entrenched communities

Some disruptive technologies are well into advanced stages of development or almost available and will certainly force us to rethink many of the assumptions and the practices informing traditional strategic stability. A list of new military disruptive technologies is, by definition, impossible to divine[9], but most analysts would probably list the following as the most prominent candidates to affect international order in the next 10-15 years: Artificial Intelligence (AI)[10] and, maybe, "quantum supremacy"[11]; autonomy, robotic systems and swarm technology; hypersonic glide systems and hypersonic cruise missiles (HGV/HCM) technologies; direct energy weapons and high energy

---

and interests that will fight tooth and nail to maintain favored programs during the downturn", S. Brimley, B. FitzGerald, and K. Sayler (2013), p. 10. See also: "The critical challenge advanced militaries face is not predicting how emergent technology will deliver decisive advantage. Rather, it is the reshaping of large military bureaucracies so that they are best postured to integrate the currently unknowable technological potential to enhance what the future fighting force can deliver in support of policy aims and objectives", M. Gilchrist, "Emergent Technology, Military Advantage, and the Character of Future War", *The Strategy Bridge*, 26 July 2018.

[9] In fact, the very same definition of "disruptive technologies" is debatable. See for instance P. Thomond and F. Lettice, "Disruptive Innovation Explored", Concurrent Engineering Conference Proceedings, July 2002.

[10] For an extensive account of AI's implications in world affairs, see: D.M. West and J.R. Allen, *How artificial intelligence is transforming the world*, Brookings, 24 April 2018.

[11] "The leak revealed that Google has achieved what Dr Preskill dubbed in his article 'quantum supremacy'. Using a quantum computer, researchers at the information-technology giant had carried out in a smidgen over three minutes a calculation that would take Summit, the world's current-best classical supercomputer, 10,000 years to execute", "Proof emerges that a quantum computer can outperform a classical one", *The Economist*, 26 September 2019. IBM response to this claim has been that, in reality, "an ideal simulation of the same task can be performed on a classical system in 2.5 days and with far greater fidelity". For a definition of quantum supremacy: "the original meaning of the term "quantum supremacy", as proposed by John Preskill in 2012, was to describe the point where quantum computers can do things that classical computers can't, this threshold has not been met", https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/

lasers; space technology; human enhancement and biotechnologies[12]. Others are in their infancy, and we still cannot foresee their potential weaponization and military use. Moreover, some disruptive technologies, like AI, are more akin to the internal combustion engine or electricity than to a weapon ("transformative technologies"), and should therefore be considered general-purpose enablers with a multitude of applications waiting to be refined, including in military affairs[13].

Cyberspace does not strictly speaking qualify as "a new technology", as it is much more: a technology-enabled domain for humans and machines to live and interact, a hypostatic abstraction, a political reality[14]. The advent of cyberspace was a game changer that added an extra layer of complexity to international relations, one which we are dangerously unprepared to cope with, and confronted us with a man-made domain in continuous technological evolution and of which we only partially understand the cultural, political and military disruptive

[12] This is, for instance, the list derived from: C.A. Bidwell, JD & B.W. MacDonald, *Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security*, Federation of American Scientists, September 2018, pp. 14-34 (other technologies included in the list comprise laser isotope separation and antineutrino detecting technologies). Candidates may vary according to the focus of the research, for instance: C. Kavanagh, *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?*, Carnegie Endowment For International Peace, August 2019; J. Kadtke and L. Wells II, *Policy Challenges of Accelerating Technological Change: Security Policy and Strategy Implications of Parallel Scientific Revolutions*, Center for Technology and National Security Policy (CTNSP), National Defense University (NDU), September 2014; Testimony before the Subcommittee on Airland of the Senate Armed Services Committee, P. Scharre, "Future of All Arms Warfare in the 21st Century", 15 March 2017.

[13] "What role will artificial intelligence play? In many ways it is too soon to tell, given uncertainty about the development of the technology. But AI seems much more akin to the internal combustion engine or electricity than a weapon. It is an enabler, a general-purpose technology with a multitude of applications. That makes AI different from, and broader than, a missile, a submarine, or a tank", M.C. Horowitz (2018), p. 39.

[14] W. Gibson, "A consensual hallucination experienced daily by billions of legitimate operators", *Neuromancer*, 1984.

implications[15]. Moreover, once AI will have been militarily applied to cyber warfare, we cannot predict the speed and level of automation at which cyber offensive capabilities will evolve[16]. AI, in fact, will introduce a whole new generation of threats[17], transforming "the character of conflict beyond information-age warfare toward 'algorithmic warfare', in the US military's phrasing, or 'intelligentized' warfare, as Chinese military thinkers characterize it"[18].

---

[15] F. Rugge, "An 'Axis' Reloaded?", in Idem (ed.), *Confronting an "Axis of Cyber"? China, Iran, North Korea, Russia in Cyberspace*, Milan, Ledizioni-ISPI Report, 2018.

[16] "Just as AI will profoundly affect the speed of warfare, the proliferation of zero day or zero second cyber threats as well as polymorphic malware will challenge even the most sophisticated signature-based cyber protection. This forces significant improvement to existing cyber defenses. Increasingly, vulnerable systems are migrating, and will need to shift to a layered approach to cybersecurity with cloud- based, cognitive AI platforms. This approach moves the community toward a 'thinking' defensive capability that can defend networks through constant training on known threats. This capability includes DNA-level analysis of heretofore unknown code, with the possibility of recognizing and stopping inbound malicious code by recognizing a string component of the file. This is how certain key U.S.-based systems stopped the debilitating "'WannaCry' and 'Petya' viruses", D.M. West and J.R. Allen (2018). See also: "While on a closer look many of the disputes could be in fact reduced to practical, procedural or technical matters, some vital legal questions remain, among them (not exhaustively): autonomous cyber capabilities and the element of intent in prohibited intervention, an autonomous system's capability to assess the severity of an incoming attack, autonomous cyber capability and the duty to take feasible precautionary measures, autonomous cyber capabilities and *mens rea* and international liability schemes for damages caused by the use of an autonomous cyber capability", R. Liivoja, M. Naagel, and A. Väljataga, *Autonomous Cyber Capabilities under International Law*, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, 2019, p. 44. See also: "One challenge could be a more efficient form of advanced persistent threat in which efforts to penetrate an adversary's computer systems employ automated capabilities with massive raw computational power that continually adjust tactics to the defenses encountered", M.E. O'Hanlon, *The role of AI in future warfare*, Brookings Institution, 29 November 2018.

[17] *Reinventing Cybersecurity with Artificial Intelligence: The new frontier in digital security*, Capgemini Institute, 2019.

[18] J.R. Allen and A. Husain, *On Hyperwar*, US Naval Institute, vol. 143, no. 7, July 2017. See also: E.B. Kania, "Great Power Competition and the AI Revolution:

It is hard to anticipate how the pace of technological innovation will unfold around the world, if a disruptive technology can be kept secret, whether liberal democracies or authoritarian regimes will foster innovation more efficiently or if disruptive technologies will emerge primarily from the private sector or from the military, or, again, if technological innovation based on defence research will offer to early adopters a critical first-mover advantage. All these variables will have significant consequences on how disruptive technologies will impact the international order. If technological innovation will be mostly commercially-driven, for instance, disruptive advances are likely to spread more rapidly to militaries around the world, hence reducing asymmetry and surprise[19]. Commercial interest might, on the other hand, hold back military development, as the private sector regularly pays much higher salaries and may drain from the public sector the human skills available (the true strategic resource for AI, just like carbon was the first industrial revolution), and it might have different views on the prospects for collaboration with the military complex. By the same token, wealthier economies might be able to invest more heavily in technological research and gain an initial advantage on which to build in order to maintain tech superiority, and drain from poorer countries the human capital needed for technological innovation and application[20]. Cyber offensive capabilities may

---

A Range of Risks to Military and Strategic Stability", Lawfare, 19 September 2017b. See also: Gen. Jack Shanahan, Department of Defense Enterprise Cloud and its Importance to the Warfighter Media Roundtable, Department of Defense Director, Joint Artificial Intelligence Center Lieut, 9 August 2019.

[19] "Moreover, if the computational power necessary to generate new, powerful algorithms prices out all but the wealthiest companies and countries, higher-end AI capabilities could help the rich get richer from a balance-of-power perspective. On the other hand, if leading militaries fail to effectively incorporate AI, the potential for disruption would also be larger", M.C. Horowitz (2018), p. 39.

[20] "The larger the change within the organization required for a military to effectively utilize new technologies, the greater the bureaucratic challenges and, with them, the likelihood that powerful countries will not have the organizational capability to adopt. This is a key mechanism through which the balance of power

also be used to illegally access research in advanced technology developed elsewhere, allowing leap-frog advances at low cost and risk. Cyber weapons, moreover, may be reverse-engineered, with the risk of proliferation of more and more cyber offensive capabilities diffused among many states and non-state actors.

The aim of this paper is to focus on the effects of disruptive technologies on international order. For analytical purposes, we will divide these effects into two distinct – but, in reality, overlapping – categories. The first is the risk that our adversaries will field a new disruptive military technology that provides them with an overwhelming military advantage they may use to our harm. In this sense, it is not the new technology *per se* that poses the greatest problem, but rather the asymmetric advantage that our adversaries receive from being the first to field it ("technological surprise"[21]). This may pave the way for painful adjustments to the international Balance of Power, with the risk even of disrupting nuclear strategic stability.

The second category of threats refers to the possibility that these disruptive technologies will fundamentally alter "the rules of the game" of international order and erode traditional nuclear deterrence principles and practices[22]. Ambiguity, entangle-

---

can change", ibid., p. 44.

[21] G.H. Heilmeier (1976).

[22] In fact, the very definition of disruptive technologies implies that we are unprepared to cope with them, for "what makes a technology" "game changing "revolutionary", "disruptive" or a "killer application" is that it both offers capabilities that were not available – and were in many ways unimaginable – a generation earlier and in so doing provokes deep questions whose answers are not readily available", S. Brimley, B. FitzGerald, and K. Sayler (2013), p. 4. See also: C. Buckley, "Disruptive Technologies", 1 October 2016. See also: "What Bloch anticipated has come to be known as a "revolution in military affairs" – the emergence of technologies so disruptive that they overtake existing military concepts and capabilities and necessitate a rethinking of how, with what, and by whom war is waged. Such a revolution is unfolding today. Artificial intelligence, autonomous systems, ubiquitous sensors, advanced manufacturing, and quantum science will transform warfare as radically as the technologies that consumed Bloch. And yet the U.S. government's thinking about how to employ these new technologies is not keeping pace with their development", C. Brose (2019), p. 122.

ment and surprise will multiply the occasions for cross-domain escalations and intertwine nuclear deterrence with deterrence in other domains, where it follows different concepts and precepts. Decision-makers will have to make existential choices in a much shorter time[23], and multiple opportunities for "use it or lose it" dilemmas will favor offensive strategies. As a result, "perfect storm" conditions for inadvertent wars will become more likely.

Disruptive technologies and asymmetric military advantage

The current atomic age's Balance of Power relies on two key conditions: nuclear survivability and Mutual Assured Destruction (MAD). Both provided strategic stability during the Cold War[24], but disruptive technologies already underway have the potential to pose a serious threat to this stability. AI will allow the real-time integration of revolutionary advances in big data analytics and data drawn from more advanced, persistent and diffused surveillance systems, which will make it easier to identify connections between discrete events. Such developments will immensely increase the capability of detecting the opponent's deployed strategic forces (such as mobile

[23] J.R. Allen and A. Husain (2017).

[24] "Changes in technology, however, are eroding the foundation of nuclear deterrence. Rooted in the computer revolution, these advances are making nu clear forces around the world far more vulnerable than before. In fact, one of the principal strategies that countries employ to protect their arsenals from destruction, hardening, has already been largely negated by leaps in the accuracy of nuclear delivery systems. A second pillar of survivability, concealment, is being eroded by the revolution in remote sensing. The consequences of pin-point accuracy and new sensing technologies are numerous, synergistic, and in some cases non-intuitive. Taken together, these developments are making the task of securing nuclear arsenals against attack much more challenging", "The New Era of Counterforce. Technological Change and the Future of Nuclear Deterrence", *International Security*, vol. 41, no. 4, Spring 2017, p. 9.

ICBMs)[25]. Coupled with increasing weapons accuracy, speed, autonomy and, perhaps, with swarm technology (also powered by AI), such developments risk threatening the hardening and the concealment of nuclear weapons and their delivery systems, therefore potentially undermining the long-term survivability of the nuclear deterrent. This will likely put nuclear strategic stability under stress[26].

In a not too distant future, moreover, cyber attacks might also allow the digital assault of nuclear facilities and arsenals[27], and might have the potential to blind space-based early-warning systems, to disable command and control centers and to disrupt decision-making processes. These developments would on the one hand stimulate the adoption of hair-trigger states of readiness and of lower level of decision making, while, on the other, they would contribute to make a disarming cyber strike a viable option[28]. Decision-making processes may also be influ-

[25] C.A. Bidwell, JD & B.W. MacDonald (2018), p. 25.

[26] A. Long, *Disruptive Technologies, Strategic Vulnerability, and the Future of Deterrence*, Saltzman Institute for War and Peace Studies, Columbia/SIPA, 2019.

[27] "A successful cyberattack on nuclear weapons or related systems – including nuclear planning systems, early warning systems, communication systems, and delivery systems, in addition to the nuclear weapons themselves – could have catastrophic consequences". Support for Cooperation among Governments to Address Cyber Threats to Nuclear Weapons Systems, Statement by The Euro-Atlantic Security Leadership Group, February 2019.

[28] "A way around this is to conceptualise the cyber challenge into: (i) a new set of capabilities that might be used and vulnerabilities that might be exploited within the computer systems and networks used across the nuclear weapons enterprise; and (ii) the broader context and environment within which nuclear policy is carried out. The former is about malware, cyber-attacks, bugs, and hacking, while the latter is about the digitised information space that all states operate in. There is even a case to be made that we should stop using the word cyber altogether, and instead revert back to the more precise language of Computer Network Attacks, Computer Network Defence, Computer/Network/Information Security, etc. More precision in terminology is undoubtedly the first step towards constructing meaningful and tailored measures to deal with specific cyber challenges in the nuclear realm", A. Futter, *Managing the Cyber-Nuclear Nexus*, European Leadership Network, July 2019. See also: "The cyber threat affects nuclear risks in at least two ways: It can be used to undermine the security of nuclear materials and

enced by the use of AI to create deep-fake media, broadcasted immediately in the information space through cyber-enabled information warfare (CEIW) campaigns in order to generate multiple competing narratives, potentially paralyzing the decision-making process or annihilating the domestic and/or allied support necessary to conduct operations in times of a potentially existential threat[29]. Of course, we are not saying that nuclear deterrence is over. But policymakers should be aware that, as technology progresses, the most basic assumptions that regulated the international order for the last decades may crumble, marking the end of "the age of easy survivability" and the beginning of "the age of vulnerability"[30].

Because technological innovation is a critical enabler of military power, the development of disruptive technologies may greatly influence the international Balance of Power even without directly impacting nuclear strategic stability[31]. The political priority given to disruptive technologies and the level of investments that is already underway in the United States, China

---

facility operations, and it can compromise nuclear command and control systems", Addressing Cyber-Nuclear Security Threats, Nuclear Threat Initiative (NTI).

[29] E.J. Moniz and S. Nunn, "The Return of Doomsday. The New Nuclear Arms Race - and How Washington and Moscow Can Stop It", *Foreign Affairs*, September/October 2019. On CEIW, see also: F. Rugge, *Mind Hacking: Information Warfare in the Cyber Age*, ISPI, 11 January 2018.

[30] "To be clear, not all nuclear arsenals have suddenly become vulnerable. But every arsenal today is less secure than it was before the computer revolution, and those countries that face stronger, richer, and more technologically sophisticated opponents will find it increasingly hard to keep their nuclear deterrents secure. The age of easy survivability is over. The age of vulnerability has begun", A. Long (2019).

[31] "The more prosaic advancements are not insignificant, however. Technological change does not have to be dramatic or sudden to create meaningful shifts in power balances or social structures. Indeed, focusing on the distant prospect of dramatic change may well distract from developing a more nuanced understanding of slower and subtler, but equally significant, changes". M.L. Cummings, H.M. Roff, K. Cukier, J. Parakilas and H. Bryce, *Artificial Intelligence and International Affairs. Disruption Anticipated*, Chatham House, 14 June 2018.

and Russia are unequivocal signs that an arm race is indeed ongoing. Russian President Putin famously declared that "[w]hoever becomes the leader in this sphere will become the ruler of the world"[32].

Progress made by China in the fields of AI[33], cyber power and HGV/HCM are, understandably, a cause for concern in the West, first and foremost because they are powerful signals of Beijing's growing power and technological edge, and secondly because they represent a powerful military deterrent at a time when China is becoming increasing assertive on the world stage. China has ambitious, yet credible goals: affirming itself on the world stage as the "premier global AI innovation center" by 2030, possibly surpassing the United States in the process[34],

[32] Weapons of the weak: Russia and AI-driven asymmetric warfare. A. Polyakova, *Weapons of the weak: Russia and AI-driven asymmetric warfare*, 15 November 2018, The Brooking Institutions.

[33] G.C. Allen, *Understanding China's AI Strategy*, Center for a New American Security, 6 February 2019. See also: "The PLA will likely leverage AI to enhance its future capabilities, including in intelligent and autonomous unmanned systems; AI-enabled data fusion, information processing, and intelligence analysis; war-gaming, simulation, and training; defense, offense, and command in information warfare; and intelligent support to command decision-making. At present, the PLA is funding a wide range of projects involving AI, and the Chinese defense industry and PLA research institutes are pursuing extensive research and development, in some cases partnering with private enterprises. This could be the start of a major shift in the PLA's strategic approach, beyond its traditional asymmetric focus on targeting U.S. vulnerabilities to the offset-oriented pursuit of competition to innovate. The PLA is seeking to engage in 'leapfrog development' (跨越 发展) to achieve a decisive edge in 'strategic front-line' (战略前沿) technologies, in which the United States has not realized and may not be able to achieve a decisive advantage", E.B. Kania (2017a), p. 4.

[34] "State Council Notice on the Issuance of the New Generation AI Development Plan" [国务院关于印发新一 代人工智能发展规划的通知], State Council, 20 July 2017. See also: "China aspires to surpass the United States in AI. The Chinese leadership recognizes and intends to take advantage of AI to enhance its economic competitiveness and military capabilities For instance, according to a recent report from PriceWaterhouseCoopers, China is expected to be one of the greatest beneficiaries of the economic contributions of AI, given an expected 26% boost to its GDP by 2030", E.B. Kania (2017a), p. 37 and p. 8. See also:

completing military modernization by 2035, and becoming a "world-class" military by 2049[35]. "China's leadership – including President Xi Jinping – believes that being at the forefront in AI technology is critical to the future of global military and economic power competition, and that China should pursue global leadership in AI technology and reduce its vulnerable dependence on imports of international technology"[36]. In this sense, it really would be impossible to draw a clear-cut distinction between Beijing's pursuit for technological (and economic) development and its national interest – and, of course, its military objectives[37].

M.E. O'Hanlon (2018).

[35] "By 2035, China's military leaders seek to complete military modernization and by 2049, they have characterized their goal as becoming a 'world-class' military. In this regard, China's efforts are designed with a clear purpose in mind: to displace the United States in the Indo-Pacific region; to expand the reaches of its state-driven economic model; and to reorder the region in its favor", C. Larson, "China's massive investment in artificial intelligence has an insidious downside", *Science*, 8 February 2018. See also: M.B. Morgan, "A 'World-Class' Military: Assessing China's Global Military Ambitions", Testimony before the US-China Economic and Security Review Commission, Office of the Secretary of Defense, Office of the Assistant Secretary of Defense for Indo-Pacific Security Affairs Acting Deputy Assistant Secretary of Defense for East Asia, 20 June 2019.

[36] "Information technology, including computers and telecommunications systems, has permeated all aspects of society and economies and become an integral part of a nation's infrastructure. Chinese analysts have dubbed this process 'informationisation (*xinxihua*; 信息化)'. From the Chinese perspective "Informationisation is a comprehensive system of systems, where the broad use of information technology is the guide, where in- formation resources are the core, where information networks are the foundation, where information industry is the support, where information talent is a key factor, where laws, policies, and standards are the safeguard". In the face of this broad trend of economic, political, and social informationisation, Chinese analysts have concluded that threats to national interests and security have also become informationised", D. Cheng, "China and Cyber: The Growing Role of Information in Chinese Thinking", in F. Rugge (ed.), (2018), pp. 59-60.

[37] "And Beijing has also smashed the barriers between civilian and military technological domains – a doctrine that China calls 'military-civilian fusion'. By law and presidential fiat, companies in China – whether private, state-owned,

In the same vein, the range of disruptive military capabilities currently under development in Russia and listed by President Putin in his famous March 2018 address to the Federal Assembly, whether realistic or not[38], are clearly intended to portray Russia as a country capable of balancing current and upcoming US military capabilities thanks to its formidable technological development[39] – such as the US Prompt Global Strike mission, which aims to develop the ability to strike targets anywhere in the world within one hour from the President's order with high-precision conventional (including hypersonic) weapons[40]. "Skyfall" is the NATO name of one of the many projects that Putin announced in 2018: an "invincible" low-flying, low-visibility nuclear-powered cruise missile armed with a nuclear warhead and nearly unlimited range and unpredictable flight path, making it "invulnerable to all existing and future anti-missile and air defense weapons"[41]. Another such capability is a nuclear unmanned underwater vehicle capable of delivering both conventional and nuclear warheads "that could outsmart all American defenses" (NATO name: "Poseidon"). In its nuclear, cobalt-bomb configuration, Poseidon's detonation along the coasts would generate towering tsunami waves capable of destroying everything up to hundreds of kilometers inland, and would contaminate that

---

or foreign – must share their technologies with the Chinese military". Remarks by the US Vice President Pence at the Frederic V. Malek Memorial Lecture, 24 October 2019, https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-frederic-v-malek-memorial-lecture/

[38] "Now we have to be aware of this reality and be sure that everything I have said today is not a bluff - and it is not a bluff, believe me", Presidential Address to the Russian Federal Assembly, 1st March 2018.

[39] "We are well aware that a number of other countries are developing advanced weapons with new physical properties. We have every reason to believe that we are one step ahead there as well – at any rate, in the most essential areas", ibid.

[40] Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues, Congressional Research Service, updated 14 August 2019.

[41] "As you no doubt understand, no other country has developed anything like this. There will be something similar one day but by that time our guys will have come up with something even better", Presidential Address to the Russian Federal Assembly, 1st March 2018, cit.

area to non-habitable conditions for decades. A third disruptive military capability that was announced by President Putin is a ground-launched hypersonic (Mach 10) cruise missile that is able to manoeuvre in all phases of its flight trajectory and can deliver within minutes and in a range of 2000 km a conventional or nuclear warhead[42]. President Putin also added two new weapons systems to the list allegedly already available to its Armed Forces: an hypersonic intercontinental missile capable of delivering a nuclear warhead at the speed of Mach 20, and a manoeuvrable hypersonic glide vehicle ("Avangard" – a Futuristic name!) that can be carried by an intercontinental ballistic missile as a multiple independently targetable reentry vehicle, travelling at an even higher speed. Russian Deputy Prime Minister Borisov stated that during the test flight of 26 December 2018, Avangard reached the incredible speed of Mach 27, or around thirty-three thousand kilometres per hour.

These new technologies (and their announces) clearly serve a political purpose in time of peace, because they confront adversaries with new and potentially divisive strategic-military challenges, and will provide a tool for intimidation and coercion in time of crisis[43], as well as a critical military advantage in times

[42] "Friends, Russia already has such a weapon. The most important stage in the development of modern weapons systems was the creation of a high-precision hypersonic aircraft missile system; as you already know for sure, it is the only one of its kind in the world. Its tests have been successfully completed, and, moreover, on 1st December of last year, these systems began their trial service at the airfields of the Southern Military District. The unique flight characteristics of the high-speed carrier aircraft allow the missile to be delivered to the point of discharge within minutes. The missile flying at a hypersonic speed, 10 times faster than the speed of sound, can also maneuver at all phases of its flight trajectory, which also allows it to overcome all existing and, I think, prospective anti-aircraft and anti-missile defence systems, delivering nuclear and conventional warheads in a range of over 2,000 kilometers. We called this system Kinzhal (Dagger)", ibid.

[43] D. Adamsky, *Cross-Domain Coercion: The Current Russian Art of Strategy*, IFRI Security Studies Center, November 2015, p. 28. See also: "The greatest danger for the United States is the erosion of conventional deterrence. If leaders in Beijing or Moscow think that they might win a war against the United States,

of war – up to the point of eventually enabling, as we have seen, a disarming first strike. For this reason, and because of the never-ending confrontation taking place in the cyber domain, it is increasingly difficult to operate in international affairs a clear distinction between the conditions of peace, crisis and war, as the three dimensions are becoming an indistinguishable continuum, and we risk providing a military response to what it is, primarily, a political challenge.

Last but not least, the asymmetric military advantage may not necessarily result from being the first to master a disruptive technology: since not all countries and non-state actors follow the same moral compass, the weaponization and first employment of a technology could be, in the end, acceptable only to one side[44].

---

they will run greater risks and press their advantage. They will take actions that steadily undermine the United States' commitments to its allies by casting doubt on whether Washington would really send its military to defend the Baltics, the Philippines, Taiwan, or even Japan or South Korea. They will try to get their way through any means necessary, from coercive diplomacy and economic extortion to meddling in the domestic affairs of other countries. And they will steadily harden their spheres of influence, turning them into areas ever more hospitable to authoritarian ideology, surveillance states, and crony capitalism. In other words, they will try, as the military strategist Sun-tzu recommended, to "win without fighting", C. Brose, (2019), p. 133. See also: "Opponent actions that stay below this threshold inhabit a "gray area," that is neither peace nor war, where the United States and its allies, unable to use military force in response, have so far been stymied in designing and articulated an effective reply. Opponents will exploit gray areas in international law to coerce without triggering armed conflict. Deterrence will be more difficult in this opaque environment, and we will see increased use by our opponents of coercive acts that fall below thresholds for the use of force or armed attack", J.A. Lewis, *Rethinking Cybersecurity. Strategy, Mass Effect, and States*, CSIS, 8 January 2018, p. 16

[44] "The U.S. military could face a disadvantage or pressures to adapt if strategic competitors such as China and Russia pursue full autonomy without similar constraints – although it remains unclear when, whether, and in what contexts greater degrees of autonomy will provide a clear advantage", E.B. Kania (2017a), p. 37. See also: J.R. Allen and A. Husain (2017).

Challenges Posed by Disruptive Technologies – Ambiguity, Entanglement, Surprise

The second category of effects on the international order posed by disruptive technologies refers to the fact that they "*immediately outdate* the policies, doctrines and organizations of all actors"[45], causing a paradigmatic shift in the way warfare is conducted[46]. This shift will likely pose unanswered questions of strategic, tactical and operational order, as well as face policy-makers with unprecedented dilemmas[47]. This shift is further complicated by the possibility that non-state actors may exploit disruptive technologies to conduct hostile operations for their own political or criminal goals, thus multiplying the possibilities for inadvertent wars. What it is more worrisome, in any case, is probably that while we start to understand what each new technology will entail, it is almost impossible to grasp the unaccountable range of unexpected emergent behaviors that could break out from the combination of the many developments underway[48].

Three major challenges related to the use of disruptive military technologies emerge on the strategic horizon: ambiguity, entanglement and surprise.

---

[45] "[w]hat are the technologies that today's naysayers derisively describe as 'science experiments' that will actually be key to shaping the battlefield of tomorrow? With the goal of exploring this question, the U.S. Department of Defense's Rapid Reaction Technology Office sponsored the NeXTech project series", S. Brimley, B. FitzGerald, and K. Sayler (2013), p. 4, italic mine.

[46] "A chicken-and-egg question has been debated within the militaries and defense industrial sectors of some nations: Does 'doctrine drive technology' or does 'technology drive doctrine'?", D.J. Blasko, "'Technology Determines Tactics': The Relationship between Technology and Doctrine in Chinese Military Thinking", *The Journal of Strategic Studies*, vol. 34 no. 3, 2011, pp. 355-381.

[47] Technological innovation is outstripping the capacity (or willingness) of technology creators, private investors, national governments, and the existing multilateral system to understand, monitor, and effectively govern the attendant effects and consequences. C. Kavanagh (2019).

[48] "The pace and complexity of technological change mean that linear predictions of current trends cannot be the basis for effective guidance or management for the future", J. Kadtke and L. Wells II (2014).

Ambiguity

Ambiguity, probably the single most distinctive feature of the cyber domain[49], is intimately connected to the concept of automation and hyperwar, where the high ("hyper") tempo of operations compresses the time available for situational awareness, recognition and decision-making[50]. Situational awareness is hampered not only because attributing cyber attacks remains a technical and intelligence challenge and false-flag operations are common, but also because high-end threats operate in the same environment of low-level skirmishes and criminal activities and share with these many technical features. Moreover, the execution of a cyber attack requires an immediate response, even if the actual scope, the real intent and the ultimate target of a cyber campaign often becomes clear – if ever – once its objectives are met.

In order to cope with the ongoing cyber malicious activity that is threatening national security interests of strategic relevance, the US Cyber Command announced in April 2018 the doctrine of "persistent engagement" with its adversaries[51]. The ultimate goal of this strategy is "to improve security and stability in cyberspace" and "to avoid escalations in the conventional domain" by "clarifying the distinction between acceptable and unacceptable behavior in cyberspace". In order to effectively engage its adversaries, the US strives to achieve "cyberspace superiority", defined as "the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space

[49] M.C. Libicki, "The Strategic Uses of Ambiguity in Cyberspace", *Military and Strategic Affairs*, no. 3, 2011. See also: "Ambiguity is the cyber domain is such that it is also disputable whether a Balance of Power in cyberspace can be assessed and maintained at all: "The question is: is a Balance of Power possible in the cyber age?"". U. Gori, "The Balance of Power in Cyberspace", in F. Rugge (ed.), (2018), p. 143.

[50] See also: R. Liivoja, M. Naagel, and A. Väljataga (2019).

[51] Achieve and Maintain Cyberspace Superiority, Command Vision for US Cyber Command, 23 March 2018, p. 6.

forces at a given time and place without prohibitive interference by an adversary". Cyber superiority allows "maneuvering seamlessly between defense and offense across the interconnected battlespace", "globally, as close as possible to adversaries and their operations", "continuously, shaping the battlespace", in order "to create operational advantage for us while denying the same to our adversaries". And, of course, cyber superiority implies a continuous technological innovation capability across the doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) spectrum.

While we never abandoned the nuclear security paradigm that postulates that "the only way to win is not to play", in the cyber domain we are drifting toward one where – so we are told – "the only way not to lose (too much) is to persistently engage the adversaries"[52]. We all subscribe to the goal of enhancing predictability in cyberspace, and, in the absence of clear and actionable international law pertaining to the behavior of states in cyberspace, it might in fact very well be that persistent operational engagement with adversaries is the only way to enhance deterrence in this "domain of ambiguity". However, the militarization of cyberspace[53], the inherent difficulty in distinguishing between the intelligence and the military nature of a campaign, the intrinsic secrecy of cyber arsenals and the massive security paradox ("my security is your insecurity") resulting from the legitimate national quests for cyber superiority, are all developments that undermine the trust within the international community and threaten the international stability, increasing the risk that misinterpretations, miscalculations and unintended escalation to the conventional domain becoming

[52] F. Rugge, *Cyberspace and the Armed Forces*, ISPI Commentary, 2 May 2018.

[53] "We recognize that adversaries already condemn US efforts to defend our interests and allies as aggressive, and we expect they will similarly seek to portray our strategy as 'militarizing' the cyberspace domain. The Command makes no apologies for defending US interests as directed by the President through the Secretary of Defense in a domain already militarized by our adversaries", Achieve and Maintain Cyberspace Superiority…, cit., p. 10.

ever more real[54]. Moreover, since messaging regarding both capabilities and intentions is intrinsically ambiguous in this domain of false-flag operations and of plausible deniability, crisis management and risk reduction are particularly cumbersome[55]. Finally, in the age of secret cyber arsenals and AI-driven algorithmic warfare, assessing each actor' relative military power

[54] "Cyber capabilities, particularly the emergence of offensive weapons, are reshaping the way policymakers in the United States think about thresholds for using force - whether provocations or attacks in cyberspace warrant a response in cyberspace or in other domains", S. Brimley, B. FitzGerald, and K. Sayler (2013), p. 20. See also: "With uncertain rules, there remains considerable potential for escalation if a conflict between two States emerges. It is also in this light that the current reluctance of States to call cyber activities such as economic espionage violations of international law can perhaps be understood", K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn, 2013, p. 216. See also J. Healey, *Triggering the New Forever War, in Cyberspace*, The Cipher Brief, 1 April 2018.

[55] "The classic example of Cold War signaling has a Soviet missile submarine move closer to the United States (this meant a shorter flight time for a missile and less warning time, which reduced stability by increasing the chance of a surprise attack). In response, the United States might visibly move bombers to a higher readiness state. Soviet reconnaissance satellites would detect this change in status, and the submarine would draw away from the coast. This kind of signaling will be difficult in cybersecurity. What would moving to a higher state of alert entail? […] A review of documents from Soviet archives made available after the Cold War shows that the deterrent message the United States thought it was sending was often not the message the Soviets received. The possibility of miscommunication exists today. Potential opponents may misinterpret signals as expressions of hostile intent, or they may discount them. The risk of misinterpretation is high", J.A. Lewis, *Conflict and Negotiation in Cyberspace*, Center for Strategic and International Studies, February 2013, p. 49. See also: "The ability to send that message requires four things: attribution (the state must be able to define the target of retaliation), thresholds (the state must be able to consistently distinguish between acts that merit retaliation and those that do not), credibility (the state's will to retaliate must be believed), and capability (the state must be able to pull off a successful response). Each of these components is exponentially more complex in cyberspace than in a conventional setting", S. Hennessey, "Deterring Cyberattacks. How to Reduce Vulnerability", *Foreign Affairs*, November/December 2017.

will be increasingly harder, making the Balance of Power more difficult to assess and enforce, and exacerbating the inaccurate perceptions of the security environment which may in turn lead to disastrous courses of action[56].

The risk of ambiguity lies also in the conventional and the nuclear domains. When faced with an incoming threat, the limited time to discriminate between a nuclear and conventional threat (warhead ambiguity) and the uncertainty about the asset under threat (target ambiguity) might in fact induce a nuclear retaliation. This is especially true if the incoming threat is perceived to be targeting the nuclear command & control system (NC2), which in turn generates "use or lose it" dilemmas for the party under attack, making an escalation more likely[57]. Because of the further compressed response time available,

[56] "Evaluation of any horizontal escalation option is subject to considerable uncertainty, especially regarding adversary perceptions, values, and escalation thresholds. Understanding how adversaries would perceive their own (much less their adversaries') stakes and risk tolerance and expected outcomes is inherently difficult. In Richard Smoke's classic ex- amination of escalation, his historical case studies show that escalation failures most often occur because of a fundamental failure on the part of policymakers to comprehend how the world looked to others and understand basic assumptions, goals, and options of decision makers in other capitals", M. Fitzsimmons, "Horizontal Escalation: An Asymmetric Approach to Russian Aggression?", *Strategic Studies Quarterly*, Spring 2019.

[57] "Analysts disagree about the strategic implications of hypersonic weapons. Some have identified two factors that could hold significant implications for strategic stability: the weapon's short time-of-flight – which, in turn, compresses the timeline for response – and its unpredictable flight path – which could generate uncertainty about the weapon's intended target and therefore heighten the risk of miscalculation or unintended escalation in the event of a conflict. This risk could be further compounded in countries that co-locate nuclear and conventional capabilities or facilities. Some analysts argue that unintended escalation could occur as a result of warhead ambiguity, or from the inability to distinguish between a conventionally armed hypersonic weapon and a nuclear-armed one", "Hypersonic Weapons: Background and Issues for Congress", Congressional Research Service, Updated 17 September 2019, p. 16-17. See also: "Yet, the president's ability to gain and maintain situational awareness during a nuclear crisis, and to clearly direct an appropriate response under extraordinarily intense time pressure is vital. As such, the United States' nuclear command and control, or

strategic forces might be regularly set on hair-trigger states of readiness, and the adoption of "launch on warning" strategies becomes likely, contributing to make the security environment highly volatile[58]. In order to prevent those dilemmas, Great Powers are already considering the space as an operational domain where to place critical enablers of their military power and where eventually to deploy pre-emptive strike capabilities – a development that does not increase predictability.

Entanglement

A second major challenge that disruptive military technologies pose to the international order is due to the increased interconnectedness and mutual dependency of nuclear and non-nuclear systems, and to the entanglements in cross-domain escalation thresholds[59].

NC2, system can be considered to be the triad's essential nervous system – without which its legs could be paralyzed. The brain directing this nervous system is provided by the president, who has the sole authority to order the launch of nuclear weapons, or to rescind such an order J.A. Winnefeld Jr., *A Commonsense Policy for Avoiding a Disastrous Nuclear Decision*, Carnegie Endowment For International Peace, 10 September 2019. See also: "There are a number of scenarios in which such missiles could inadvertently increase the chance of a nuclear war. The most obvious is that in a conflict, they might be launched with conventional warheads but mistaken for nuclear weapons. This ambiguity could prompt the adversary to launch an immediate nuclear response. It is difficult to know whether it would choose this course of action – or wait until the weapons had detonated and it became clear how they were armed", J.M. Acton, *The Weapons Making Nuclear War More Likely*, Carnegie Endowment For International Peace, 8 February 2019.

[58] "While much attention has been focused on renewed U.S. interest in potentially deploying space-based interceptors, another concept that emerged from President Ronald Reagan's Strategic Defense Initiative in the 1980s is also being reexamined: putting lasers or neutral particle beams in space to shoot down enemy missiles", J. Harper, "SPECIAL REPORT: The Pentagon Could Put Directed Energy Weapons in Space", National Defense, 25 April 2019. See also: R.H. Speier, G. Nacouzi, C.A. Lee, and R.M. Moore, *Hypersonic Missile Nonproliferation. Hindering the Spread of a New Class of Weapons*, RAND Corporation, 2017, p. 47.

[59] "Not only has the United States' ability to deter aggression in the traditional

As a result of the increased physical and logical interconnectedness and mutual dependency of nuclear and non-nuclear systems, an attack against Intelligence, Surveillance and Reconnaissance (ISR) or nuclear early-warning systems could exacerbate the risk of a nuclear overreaction[60], because it would complicate the task of assessing an attacker's intent, and could

---

air, land, and sea domains of warfare been cast in doubt, but new requirements to deter future aggression in the domains of space and cyberspace have also arisen. When an opponent has no incentive to initiate or escalate conflict at any given intervention or escalation threshold in any given domain of warfare – both vertically and horizontally within that domain and laterally into one or more additional domains of warfare – successful cross-domain deterrence can be said to be in effect", K. Mallory, *New Challenges in Cross-Domain Deterrence*, RAND Corporation, 2018.

[60] *Nuclear Weapons in a New Geopolitical Reality. An Urgent Need For New Arms Control Initiatives*, Adviesraad Internationale Vraagstukken, no. 109, January 2019, pp. 40-41. See also: "Entanglement has various dimensions: dual-use delivery systems that can be armed with nuclear and non-nuclear warheads; the commingling of nuclear and non-nuclear forces and their support structures; and non-nuclear threats to nuclear weapons and their associated command, control, communication, and information (C3I) systems. Technological developments are currently increasing the entanglement of non-nuclear weapons with nuclear weapons and their enabling capabilities", A. Arbatov, V. Dvorkin, P. Topychkanov, and Tong Zhao Li Bin, *Entanglement. Russian And Chinese Perspectives on Non-Nuclear Weapons and Nuclear Risks*, Carnegie Endowment for International Peace. See also: "[…] increasingly, these nuclear command-and-control systems are also being used to support non-nuclear operations. The U.S., for example, operates satellites to provide warning of attacks with nuclear-armed or conventionally armed ballistic missiles. In a conflict between NATO and Russia, these could be used to detect short-range conventional ballistic missiles launched by Russia – as the first step towards shooting them down. If this strategy was successful, Russia could decide to attack the US early-warning satellites in response. In fact, the US intelligence community has warned that Russia is developing ground-based laser weapons for that exact purpose. But blinding US early-warning satellites would not simply undermine its ability to spot conventionally armed missiles. It would also compromise the ability of the US to detect nuclear-armed ballistic missiles and could raise fears that Russia was planning a nuclear attack on the US", J.M. Acton (2019); and Idem, "Escalation through Entanglement. How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War", *International Security*, vol. 43, no. 1, Summer 2018, p. 97.

impair the effectiveness of the retaliatory capability. The 2018 US Nuclear Posture Review makes it clear that the "United States would only consider the employment of nuclear weapons in extreme circumstances […] includ(ing) attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities"[61]. This is particularly worrisome given the ever-increasing reliance of modern warfare on the cyber domain and on the security of space, where critical parts of the nuclear early-warning system reside and where any initiative aimed at acquiring military dominance in the early stage of a conflict would probably start[62].

[61] *US Nuclear Posture Review*, February 2018, p. 21.

[62] "The emergence of precision-guided munitions drove war's center of gravity into space. Other causes came later, but space became indispensable for managing Precision-guided munitions (PMGs), and any serious war has to begin there. If the U.S. and China ever go to war, the Chinese will need to fire PGMs at American ships, and therefore the Americans must blind them before they can do that by destroying China's space-based system", G. Friedman, "George Friedman's Thoughts: War and a New Geopolitical Age", *Geopolitical Futures*, 3 October 2019. See also: "The U.S. Air Force and U.S. Space Command, in partnership with industry, are developing options to field the sensors, shooters, and command and control nodes required to fight in, through, and from space by engaging targets. But the development of space-minded warfighters is the best way to make joint space operations more credible and responsive by both enabling and increasing the lethality of multidomain operations, or what the Joint Staff now calls "joint all-domain command and control", R. Agrawal and C. Fernengel, "The Kill Chain In Space: Developing A Warfighting Mindset", *War on the Rocks*, 24 October 2019. See also: "The implications of this logic are not limited to the cyber domain. Nor are they limited to Russia, China being as much a concern in this regard as well. There will be strong incentives in a serious crisis for China to initiate and rapidly escalate attacks against U.S. space infrastructure. While China may not wish to initiate such attacks, it could feel compelled to strike in space before the United States does, rather than risk the far more dangerous alternative of striking second. This same dynamic is pertinent in the cyber domain as well as the space domain. In short, the world faces a new and highly dangerous pressures where, even if the dynamics of the environment are understood at a given point in time, technological change could easily upend that new understanding in a relatively short time", C.A. Bidwell, JD & B.W. MacDonald (2018), p. 7. See also: "The focus here is principally on conventional military operations. Cyber, counterspace, financial, information, and other tools

Nuclear escalations resulting from entanglement is also the result of technological innovations in the field of dual-use missile technologies[63]. China, for instance, "has chosen to mount both conventional and nuclear warheads on the same missiles and to attach both conventional and nuclear launch brigades to the same bases. It likely sees some strategic advantage in these linkages. Precisely because these entanglements raise the prospect of nuclear escalation, Beijing may believe that they contribute to deterrence – that they will make the United States less likely to go to war in the first place"[64]. The Russian dual-use, short and medium range ground-launched cruise missile 9M729, for which Washington declared Moscow non-compliant with the

---

should be profitably analyzed in the context of asymmetric deterrence and escalation management. However, they would likely be employed in any response to Russian aggression and do not fit comfortably in the framework of horizontal escalation", M. Fitzsimmons (2019).

[63] Other processes underway are the rapid expansion of cyber warfare technology, the militarization of space, and modernization of missile defense systems, which are gaining offensive (including anti-satellite) capabilities. Many offensive weapons have dual use, and it will be impossible to distinguish them from nuclear ones until an actual impact. Such weapons and automated command-control and information systems could trigger an uncontrollable escalation of a local conflict. Incidentally, this danger was implicitly exposed by Russian Defense Minister Sergei Shoigu when he said: "With the current level of automation and informatization, there is a high probability of error in the command-control system over the military forces". At the same time, concepts and means of conducting a limited nuclear war are eroding the "nuclear threshold," a danger recently mentioned by Russian President Vladimir Putin", A. Arbatov, *A New Era of Arms Control: Myths, Realities and Options*, Carnegie Moscow Center, 24 October 2019.

[64] C. Talmadge, "Beijing's Nuclear Option. Why a U.S.-Chinese War Could Spiral Out of Control", *Foreign Affairs*, November/December 2018. See also: "In practice, the greatest danger with dual-use missiles may lie elsewhere: misidentification before they have even been launched. Imagine that China dispersed lorry-mounted DF-26 missiles loaded with nuclear warheads around its territory. The U.S., wrongly believing them to be conventionally armed, might decide to try to destroy them. By attacking them, it could inadvertently provoke China into launching those nuclear weapons it still had before they could be destroyed", J.M. Acton (2019).

provisions of Intermediate-Range Nuclear Force (INF) Treaty, is a proof of how nuclear and non-nuclear systems are increasingly entangled globally, making the risk of inadvertent nuclear escalation more likely.

Nuclear threat notwithstanding, hypersonic vehicles will probably blur the distinction between conventional and strategic weapons due to their speed and manoeuvrability, which drastically decrease response time and create unpredictable flight paths that make air defences ineffective. Hypersonic technologies reintroduce decapitation as a viable attack strategy, as a single strike can critically disrupt the nuclear decision-making chain of command and destroy critical components of the adversary's NC2. This, in turn, may induce the devolution of strategic forces' command and control to lower levels of authority[65]. Faced with an incoming hypersonic threat, policy-makers could therefore still view such a weapon as "strategic in nature" (keeping also in mind the quasi nuclear-equivalent kinetic energy released at impact by HGV/HCM[66]) regardless of the

[65] R.S. Cohen, "Hypersonic Weapons: Strategic Asset or Tactical Tool?", *Air Force Magazine*, 5 July 2019. See also: "Prime targets could include destroying a nation's leadership and command and control, referred to as 'decapitation', to prevent the target nation from responding with an effective follow-on attack. […] Any government faced with the possibility that hypersonic missiles would be employed against it – particularly in a decapitating attack – would plan countermeasures, many of which could be destabilizing. For example, countermeasures could include devolution of strategic forces' command and control so that lower levels of authority could execute a strategic strike, which would obviously increase the risk of accidental strategic war; or strategic forces could be more widely dispersed – a tactic risking greater exposure to subnational capture. An obvious measure would be a launch-on-warning posture – a hair-trigger tactic that would increase crisis instability. Or the target nation could adopt a policy of preemption during a crisis - guaranteeing highly destructive military action", R.H. Speier, G. Nacouzi, C.A. Lee, and R.M. Moore (2017), p. 17.

[66] "Hypersonic weapons can deliver nuclear or conventional warheads. However, another attribute common to both HCMs and HGVs is the potential to use solely kinetic energy to destroy or damage an unhardened target. This is made possible by the combination of their high speed, or kinetic energy, and their accuracy", R.H. Speier, G. Nacouzi, C.A. Lee, and R.M. Moore (2017), p. 13.

actual payload and of the intent of the State firing the weapon, and could consider that a nuclear response is appropriate. Differences in threat perception and escalation ladders could thus exacerbate the risk of an unintended escalation[67].

The pervasive nature of the cyber domain makes entanglement one of its essential features. In fact, when the Russians first started to explore "the science of cybernetics" (kibernetika), it was "seen as a discipline in the intersection of exact, social, and natural sciences. Soviet scientific society defined cybernetics as science exploring the nature of creation, storage, transformation, utilization, and management of information and knowledge, in complex systems, machines, contiguous living organisms, or societies"[68]. Entanglement in cyberspace also results from the multitude of public and private stakeholders sharing the same infrastructure, technologies and technics: global actors are already aware of the potential destabilizing role that non-state actors (state-supported hacking communities, transnational organized cybercrime, hacktivists…) may play in international relations[69].

Some have questioned whether the increasing financial, economic, political, technological interconnections that hold the world together have instead a stabilizing effect in international relations by making it impossible for an actor to impose a cost on an adversary without sustaining equivalent harm. Professor Joseph Nye, for instance, has argued that the interconnected nature of cyberspace and the infinite global mutual

[67] Congressional Research Service, August 2019, p. 17.

[68] D. Adamsky (2015). On the Russian interest for "kibernetika" see also: A. Klimburg, *The Darkening Web. The War for Cyberspace*, Penguin Press, 2017, pp. 207-209.

[69] "Private entities, due to their deep involvement and tasks they perform in cyberspace, exacerbated by the dual use of cyber infrastructure, can face entanglement in interstate conflicts. Because of the crucial role of these entities in keeping the Internet up and functioning, they should be afforded protected status", J. Healey, J.C. Mallery, K. Tothova Jordan, and N.V. Youd, *Confidence-Building Measures In Cyberspace. A Multistakeholder Approach for Stability and Security*, Atlantic Council, November 2014, p. 14.

dependencies that characterize modern societies imply that the costs of a cyber attack would exceed its benefits ("deterrence by entanglement")[70]. It is possible that AI will make mutual dependencies among the systems supporting national complexes so critical, weapons' automation so deadly and decision-making so immediate that the idea of war will become simply irrational, because the risks of a nuclear Armageddon would become unbearable[71]. But even in this case, there would always be the possibility that a cybercrime campaign or a disruptive attack to critical infrastructure by hacktivists or "cyber patriots" would be misinterpreted as the beginning of a hybrid military campaign, and would therefore trigger an unintended escalation[72].

---

[70] J.S. Nye, "Can Cyber Warfare Be Deterred?", *Project Syndicate*, 10 December 2015. Nye has developed these ideas in his essay, "Deterrence and Dissuasion in Cyberspace", *International Security*, vol. 41, no. 3, Winter 2016/17, pp. 58-60. See also: G. Perkovich and A.E. Levite (eds.), *Understanding Cyber Conflict. 14 Analogies*, Washington DC, Georgetown University Press, 2017, p. 170. See also: "Entanglement refers to the existence of various interdependences that make a successful attack simultaneously impose serious costs on the attacker as well as the victim". J.S. Nye Jr. (2016/17), p. 58.

[71] "In 1898, a Polish banker and self-taught military expert named Jan Bloch published *The Future of War,* the culmination of his long obsession with the impact of modern technology on warfare. Bloch foresaw with stunning prescience how smokeless gunpowder, improved rifles, and other emerging technologies would overturn contemporary thinking about the character and conduct of war. (Bloch also got one major thing wrong: he thought the sheer carnage of modern combat would be so horrific that war would "become impossible")", C. Brose (2019), p. 122. See Also: "Above all, overconfidence about the decline of war may lead states to underestimate how dangerously and quickly any clashes can escalate, with potentially disastrous consequences. It would not be the first time: the European powers that started World War I all set out to wage limited preventive wars, only to be locked into a regional conflagration. In fact, as the historian A. J. P. Taylor observed, "every war between Great Powers . . . started as a preventive war, not a war of conquest." A false sense of security could lead today's leaders to repeat those mistakes", T.M. Fazal and P. Poast, "War IS Not Over. What the Optimists Get Wrong About Conflict", *Foreign Affairs*, 15 October 2019.

[72] "Cyber operations generally are not affected by physical space, but geographic proximity matters on the Korean peninsula. In the case of a crisis or conflict in Korea, escalation dynamics easily could spill across war-fighting domains.

On the other hand, future cyber weapons and "algorithmic warfare" brought by AI[73] will probably be able to mitigate collateral damage and only strike very specific targets, which would limit the stabilizing effects of deterrence by entanglement – while, at the same time, not avoiding the risks of a voluntary cross-domain escalations[74].

Misperception of an adversary's intent, or miscalculation surrounding capabilities and likely outcomes could create strong incentives to strike first in an effort to avoid unacceptable consequences", D.A. Pinkston, "North Korean Cyber Threats", in F. Rugge (2018), p. 89. See also: "The risk of any one incident or set of circumstances leading to escalation is greatly exacerbated by new hybrid threats, such as cyber risks to early warning and command and control systems. Cyber threats can emerge at any point during a crisis and trigger misunderstandings and unintended signals – magnified by the difficulties in attribution and real-time attack assessment – that could precipitate war", Support for Crisis Management Dialogue and Strategic Stability in the Euro-Atlantic Region, Statement by The Euro-Atlantic Security Leadership Group, February 2019.

[73] "Dominance in A.I. is not a question of software engineering. But instead, it's the result of combining capabilities at multiple levels: code, data, compute and continuous integration and continuous delivery. […] In this future high-end fight we envision a world of algorithmic warfare and autonomy where competitive advantage goes to the side that understands how to harness 5G, A.I., enterprise cloud and quantum, when quantum's available, into a viable operational model, all part of the department's transformation from a hardware – hardware-centric to an all-domain digital force. This digital more – modernization is a war-fighting imperative that demands a palpable sense of urgency, and it's one that will be fueled by an enterprise cloud solution", Gen. Jack Shanahan (2019).

[74] "Some kinds of cyber attacks, such as the destruction of servers or other network devices, or of critical infrastructure providing service to a broad population, pose greater risk of collateral damage, but these only provide limited military advantage. One implication of this is that the benefits of "entanglement" can be overstated. Entanglement is the idea that opponents will be deterred from launching cyber attacks because they will experience harm as well as the target. But since the most damaging weapons are also the most precise, entanglement will not restrict their use", J.A. Lewis (2018), p. 19.

Surprise

A third major challenge that disruptive military technologies pose to the international order results from the exponential increase in opportunities for strategic surprise: the combined employment of these new technologies will determine unexpected emergent behavior that will impact international security in unintended and unforeseeable ways, contributing to making the strategic environment more unpredictable and hence volatile.

What we do know about future warfare is already sufficient to expect a paradigmatic shift in how future wars will be fought. The concept of "hyperwar" was developed to describe the accelerated operational tempo of future warfare, where automated decision-making and the concurrency of action enabled by both AI and machine cognition will determine the collapse of the decision-action cycles to fractions of a second[75]. While we are certainly not ready for fighting such a war, we also seem unprepared to grasp the strategic, operational and moral implications of this revolution[76]. If on the one hand, in order to help us understand them, AI will assist our decision-making by bringing into play the computational power necessary to

[75] "In military terms, hyperwar may be redefined as a type of conflict where human decision making is almost entirely absent from the observe-orient-decide-act (OODA) loop. As a consequence, the time associated with an OODA cycle will be reduced to near-instantaneous responses. The implications of these developments are many and game changing. […] The hyperwar these technologies will enable is a new paradigm for which we need to plan. The rise of these capabilities has sparked a revolution. But it is more than a revolution in military affairs, it is a revolution in human affairs with major implications for the security and defense arenas. Advances in AI have the capability to fundamentally change the human condition, and with it, a profoundly human undertaking, war", J.R. Allen and A Husain (2017).

[76] "In today's tech-crazed world, where many of us see technological solutions (e.g., disruptive technologies) as a panacea to just about anything, defense analysts have a tendency to overestimate the impact of technological changes and new innovations on warfare", F.-S. Gady, "'The Fog of Peace': Why We Are Not Able to Predict Military Power. Our obsession with technology can pose problems in doing good analysis", *The Diplomat*, 4 February 2015.

instantly process great quantities of relevant data and reducing ambiguity and the fog of war, on the other hand we cannot weigh the conditions that will have to be met to ensure the reliability of these AI-assisted decision-making processes. Will our opponents, for instance, be able to manipulate the data used for our AI-assisted decision-making, hacking outcomes to their advantage[77]?

We also do not know to which extent the operational requirements of fighting such an accelerated warfare could force military planners to take humans out of the decision-making process ("out of the loop"). This of course brings into play an entirely new moral and strategic set of issues[78]. If automation becomes a decisive factor for military superiority, we might then expect to see an international race to push humans "out the loop" – a race that will not necessarily revolve around moral values. One wonders whether, in the age of AI and automation, there will still be time for a human in-the-loop to apply some common sense in the case of future disruptions or malfunctioning of AI-operated critical military systems, the kind of

[77] "Simply put, artificial intelligence can give decision-makers a lot of tools to prevent them from 'suppress(ing) alternative stories' or falsely producing 'a single coherent interpretation of what is going on around us', as Daniel Kahneman reminds us", M. Karlin, *The implications of artificial intelligence for national security strategy*, Brookings, 1 November 2018. See also: "The increasing capability of artificial intelligence will influence all three phases of national security strategy formulation: diagnosis, decision-making, and assessment. Indeed, it likely will both facilitate and impede them", ibid.

[78] "Perhaps of greatest concern is the inability of machine-learning systems to explain the logic behind the conclusions they reach. Critically, the potential inability of humans to understand machine decision-making criteria for the use of force offers ethical challenges unique in the history of warfare", M. Gilchrist (2018). See also: "Today, decision-makers in Washington and Moscow have only a precious few minutes to decide whether a warning of a possible nuclear attack is real and thus whether to retaliate with a nuclear attack of their own. New technologies, especially hypersonic weapons and cyber attacks, threaten to make that decision time even shorter. Such shrinking decision time and heightened anxieties make the risk of a mistake all too real", E.J. Moniz and S. Nunn (2019), p. 158.

common sense shown by the Russian Col. Petrov in the night of 26 September 1983, when he refused to launch a nuclear retaliation in response to what later proved to be a technological glitch of what was then a state-of-the-art early-warning system. Surprise, in a sense, will also be an everyday experience for humans, once they will be assisted in every aspect of their life (warfare included) by AI, whose decision-making processes are cognitively inaccessible to humans[79].

Another element of surprise – and, hence, unpredictability – in international security will depend on the impact of non-state actors on the future automated digital military environment. Since 9/11 we have been reminded of the critical impact that non-state actors can play in international relations, and it is quite possible that future technologies will enable an even greater role of non-state actors (private companies, transnational organized crime, terrorists,…) in R&D, distributed sensoring, collective emergent behavior and so on. What will for instance be the role of the future Googles and Apples in enabling states' military power, or in providing technological enablers to non-state actors[80]? Will collaborative engagement techniques, enabled by swarms technologies and AI, empower disperse adversary groups of individuals to act in conjunction,

[79] "General Paul J. Selva, Vice Chairman of the Joint Chiefs of Staff, coined the phrase 'Terminator Conundrum' to describe dilemmas associated with autonomous weapons, and he has reiterated his support for keeping humans in the loop because he 'doesn't think it's reasonable to put robots in charge of whether we take a human life'. However, the U.S. military could face a disadvantage or pressures to adapt if strategic competitors such as China and Russia pursue full autonomy without similar constraints – although it remains unclear when, whether, and in what contexts greater degrees of autonomy will provide a clear advantage", E.B. Kania (2017a), p. 37.

[80] "Employees at Google and Microsoft have objected to their companies' contracts with the Pentagon, leading Google to discontinue work on a project using to analyze video footage. China's authoritarian regime doesn't permit this kind of open dissent. Its model of "military-civil fusion" means that Chinese technology innovations will translate more easily into military gains", P. Scharre, "Killer Apps. The Real Dangers of an AI Arms Race", *Foreign Affairs*, May/June 2019.

inflicting massive damage?[81] The truth is: we do not know what the future will bring – but it will certainly provide surprises that risk triggering unintended escalations.

The destabilizing effects of disruptive technologies is aggravated by the fear that our adversaries may be actively engaged in their clandestine development. This fuels distrust in the international community and provides fertile ground for misperceptions regarding signaling in time of crisis[82]. Conversely, clandestine development might result in a misleading sense of superiority, and put pressure upon policy-makers to use the technology they just developed so as not to lose the advantage of surprise[83]. Cyber weapons, also, risk becoming obsolete once

[81] "In congressional testimony in October, Attorney General Jeff Sessions was pressed on whether the administration had done enough to prevent Russian interference in the future. "Probably not", Sessions said. "And the matter is so complex that for most of us we are not able to fully grasp the technical dangers that are out there", G. Miller, G. Jaffe, and P. Rucker, "Doubting the intelligence, Trump pursues Putin and leaves a Russian threat unchecked", *The Washington Post*, 14 December 2017.

[82] "Many of these capabilities for locating and striking nuclear targets must remain secret in order to be effective, which constrains the ability of leaders to accurately perceive the nuclear balance and pursue appropriate strategies of deterrence and assurance. This combination – of revolutionary and increasingly clandestine technologies – means that neither non- governmental analysts (who are generally unaware of the changes) nor government officials (whose work on strategic systems is highly classified and compartmentalized) have adequately explored the military and political implications of the new era of strategic vulnerability", A. Long (2019).

[83] "Use of AI, big data analytics, and persistent surveillance can give a nation's leadership the sense that they have superior and more detailed knowledge of an adversary's capability and intentions. This feeling of information superiority can create a sense of perceived advantage. When one party perceives itself as having such knowledge superiority, it may lead them to the conclusion that they can initiate a first strike attack. At the same time, if a nation's leadership perceives that it is at risk of falling well behind an adversary in these critical technologies, whether or not it is true, that leadership could in a crisis fell more compelled to escalate and strike first than it would if it had no such concerns. Either way, this leads to a more unstable world at greater risk of escalation to nuclear war", C.A. Bidwell, JD & B.W. MacDonald (2018), p. 35.

zero-day vulnerabilities are patched, generating upon the developer a classic "use it or lose it" dilemma.

The fear of being caught by surprise has another perverse effect: it provides incentives to field newly-developed responses to military requirements without a proper test run. This already happens every day in cyberspace, where cutting corners on safety is the norm in order to shorten time to market[84]. Conversely, the meticulous application of "security by design" principles might direct AI systems to implement by default very effective self-defense preventive strategies, resulting, at the systemic level, in "creeping escalations" and brinkmanship.

Conclusion

Considering the military advantage that future disruptive technologies could bring (and all the related unknowns), it is understandable that attaining technological supremacy ranks as a top national security priority among the leading international Powers. This urgency, however, also seems to reflect the deterioration of the international security environment and the growing distrust around international collaborative approaches, and the return (from the times of the Futurists) of the idea that, in the words of the latest National Security Strategy of the United States, "sovereign states are the best hope for a peaceful world"[85].

---

[84] "For each country, the real danger is not that it will fall behind its competitors in AI but that the perception of a race will prompt everyone to rush to deploy unsafe AI systems. In their desire to win, countries risk endangering themselves just as much as their opponents. […] Digital security is already too often an afterthought. A world of widespread, unprotected AI systems isn't just a possibility; it's the default setting", P. Scharre (2019), p. 135 and p. 143.

[85] "This strategy is guided by principled realism. It is realist because it acknowledges the central role of power in international politics, affirms that sovereign states are the best hope for a peaceful world, and clearly defines our national interests. It is principled because it is grounded in the knowledge that advancing American principles spreads peace and prosperity around the globe. We are guided by our values and disciplined by our interests", White House, *National Security Strategy of the United States of America*, Washington DC, pp. 34-35.

In this context, the urgency surrounding disruptive technologies also sounds like a call to arms, a way of reestablishing a culture of readiness as a part of the wider efforts to strengthen the deterrence and defence postures to contain international actors that are increasingly assertive at the global level, and that are competing for the first time in centuries with the West in the development of cutting-age technology[86]. Historical analogies might often be misleading, but today's hype around disruptive technologies, the urgency to expeditiously proceed with the decoupling of the global ICT supply chain following security concerns (for instance in 5G technologies) and the renewed attention to dual-use export controls and foreign investments issues all remind us of the West's response to the shock produced by the Soviet Union's launch of an Intercontinental Ballistic Missile (ICBM) in January 1958 and its launch of the world's first satellite, Sputnik. In the US, these events led to the creation of the Defense Advanced Research Projects Agency (DARPA)[87]. The attempt of NATO to raise Allies' awareness and to give priority to the maintenance of the Alliance's technological superiority seem to follow the same logic.

The ongoing race to attain technological supremacy is taking place at a time when nuclear strategic stability relies on nuclear balance and the MAD paradigm. The two are not in contradiction, but there are many ways in which they may collide in the future. In this sense, "the biggest danger […] in an arms race is not losing, but creating a world in which no one wins"[88]. The

[86] M. Strout, *Pentagon Official Says America Must Join an Arm Race in Weaponry with Artificial intelligence*, The Center for Public Integrity, 11 April 2018.

[87] G.H. Heilmeier (1976). See also: M.I. Handel, "Surprise and Change in International Politics", *International Security*, vol. 4, no. 4, Spring, 1980, pp. 57-85.

[88] "Today, the United States should work with both allies and adversaries to boost international funding on AI safety. It should also begin discussions with China and Russia over whether some applications of AI pose unacceptable risks of escalation or loss of control and what countries can do jointly to improve safety. The biggest danger for the United States in an arm race is not losing but creating a world in which no one wins", P. Scharre (2019), p. 144. See also: "'Arms race stability'. In this concept, there is an absence of perceived or actual incentives to augment a nuclear force – qualitatively or quantitatively - out of the fear that

extremely low awareness among policy-makers, civil society and public opinion (and, in particular, the younger generations) of the risks implicit in the ongoing technological race is therefore particularly worrisome. In particular, developing a comprehensive understanding of how the ongoing confrontation in cyberspace affects international stability and links together the political, military, economic and sociological spheres (in other words, updating George Kennan's "X telegram" to reflect the new strategic horizon brought about by the confrontation in cyberspace) would be critical in enhancing the mutual comprehension of deterrence postures in cyberspace, and therefore in making it easier to develop confidence-building measures, to draw clear red lines and to establish well-recognized thresholds for retaliation in cyberspace and, eventually, to manage risk-reduction for cross-domain escalations[89].

---

in a crisis an opponent would gain a meaningful advantage by using nuclear weapons first. When an offsetting weapon itself poses a sufficiently compelling threat to one country, it could well stimulate that country to deploy another offsetting weapon, and so on in a repeating action-reaction cycle that can be both expensive and destabilizing to all countries involved", C.A. Bidwell, JD & B.W. MacDonald (2018), p. 25.

[89] "In the Cold War, the US and USSR brought to bear all instruments of national power – economic, military, scientific and technological. In particular, the Mr. X telegram developed by George Kennan at the start of the Cold War outlined a comprehensive strategy where the US was able to bring all elements of its national power together toward a common objective, the containment of the USSR. A key predicate of that telegram was that conflict was inevitable between the two powers, and the US required a proactive, comprehensive strategy to prepare for the characteristics of this new conflict. Given the new order being created in cyberspace – where the Internet touches all aspects of political, military, economic, and sociological life – perhaps one of the most important lessons from the Cold War is the idea of developing a Mr. X-like telegram for cyberspace that defines the boundary conditions for future conflict", D. Sulek and N. Moran, *What Analogies Can Tell Us About the Future of Cybersecurity*, Ios Press, 2009. See also: "In a speech delivered in Alabama in 1963, Martin Luther King affirmed "Injustice anywhere is a threat to justice everywhere. We are caught in an inescapable network of mutuality, tied in a single garment of destiny. Whatever affects one directly, affects all indirectly". I believe that this statement, which embodies the highest moral authority of the US civil rights' movement, perfectly

The explosive growth of technological innovation is undercutting the capacity both of national governments and of the International Community to understand and effectively govern the ongoing technological revolution. The governance gap in international relations that is constraining the development of collaborative approaches to regulate the race in disruptive technologies is the same governance gap that has emerged so forcefully in cyberspace, where a perpetual conflict is underway and the legitimate quest for cyber superiority is resulting in a growing security paradox. This global race will permeate the business competition of the future and further divide nations based on their ability to capture these gains in a competitive global landscape[90]. But the reasons that make this race so competitive underscore the need for renewed efforts by the International Community to develop common approaches and work for the development of a binding regime of arms control[91]. This would be in the interest of both the more advanced states and those that lag behind in the race, in order to prevent the historical trap in which an overwhelming military advantage is sooner or

describes one of the most critical challenge of our generation: that of ensuring a secure and just order in cyberspace", F. Rugge (ed.) (2018), p. 35.

[90] M.C. Horowitz (2018).

[91] "New production technology will be used to modernize industrial tools used in the production of 'old' and 'mature' technology, especially the production of propellant, casings, subcomponents, (notably electronic components), enabling higher reliability and enhanced performances. Extensive use of these means of production by industrialized countries will also dramatically decrease the cost of production, impacting national acquisitions and exports. Assessing to what extent such technology could enable the acquisition of production lines for ballistic and cruise missiles is of utmost interest. The problem of dissemination should not only be perceived through the threat of long-range, intermediate and intercontinental missiles but also through the prism of short- and medium-range systems, ballistic or not, easy to produce and market and which will become ordinary parts of military inventories. In this perspective, traditional instruments of control are still useful but potentially insufficient and should be completed by political instruments", "Capturing technology, rethinking arms control", Reader of the March 2019, Conference organized by the German Ministry of Foreign Affairs, p. 36.

later exploited. In the age of nuclear entanglement and automation, such a conflict could easily be our last[92].

In order to regulate the race in disruptive technologies and to ensure the stability of cyberspace, renewed political and diplomatic efforts are desperately needed, and a greater diversity of actors should be involved to shape and regulate technical and normative solutions[93]. In addition to developing these new technological capabilities at the speed of relevance in order to maintain a credible deterrent, it is important to recognize that

---

[92] "Although the push for leapfrog developments marks a continuation of previous policy, there are strong concurrent indications that Chinese officials are also concerned about AI causing an arms race and potential military escalation. Statements of senior officials seem to suggest a belief in cooperation and arms control in order to mitigate the risks that AI's military development poses", H. Roberts, J. Cowls, J. Morley, M. Taddeo, V. Wang, and L. Floridi, *The Chinese Approach to Artificial Intelligence: an Analysis of Policy and Regulation*, SSRN Paper, 23 October 2019, p. 7.

[93] "Technological innovation is largely taking place beyond the purview of governments. In many cases, the rate of innovation is outpacing states' ability to keep abreast of the latest developments and their potential societal impacts. And even if one or a handful of national governments devise policies for managing these effects, the global reach of many emerging technologies and their impacts requires new approaches to multilateral governance that are much more difficult to agree on. A greater number and variety of actors must be involved to initiate, shape, and implement both technical and normative solutions", C. Kavanagh (2019), p. 5. See also: "Cyberspace has become, and will most likely increasingly be, an environment characterized by an 'unthinkable complexity', where a multitude of diverse players constantly connect throughout the globe generating "an inescapable network of mutuality". As such, scholars will have to investigate whether the cause of order in the cyber domain might be served more appropriately by – and better understood, from the analytical point of view, with – a not state-centric approach" […] Maybe it is by following Grotius steps and by looking at cyberspace as an hypostatic abstraction of its own, with its own peculiar functioning norms and principles and with a set of authorities that include sovereign states along with many others, that it would be possible to overcome the limits intrinsic in a purely state-centric approach in cyberspace. What appears to be certain is that enforcing an order that does not reflect the complexity of cyberspace will be more and more difficult, especially given the speed of the technological revolution underway", F. Rugge, "An 'Axis' Reloaded?", in Idem (ed.) (2018), p. 35-37.

no international actor fully grasps the security implications of the emerging security environment, and that we are drifting into it without the "safety nets" that helped us manage the nuclear risk during the Cold War, such as an in-depth awareness among policy-makers and the public opinion about the risks associated with nuclear stability, the predictability provided by international arms reduction treaties, and the existence of reliable communication channels between all relevant stakeholders for defusing a potential crisis. It is therefore urgent to invest at the institutional level, bringing into play political and diplomatic skills and tools to forge common approaches and regulations and to foster cooperation between states and within international organization and multi-stakeholders regimes.

2. Disruptive Technologies in Military Affairs

Gabriele Rizzo

We are observing a democratization of technology: increasingly capable devices are more and more readily available at lower and lower prices. For instance, the cost of DNA sequencing shrank from $2.7 billion to $1,000 between 2000 and 2017. Similarly, from 2009 to 2014, the costs of 3D Lidar sensors fell from $30,000 to just $80[1]. On the other, "software is eating the world": digital technologies – and software capabilities more in general – are quickly becoming the major source of value creation[2]. "Uber, the world's largest taxi company, owns no vehicles. Facebook, the world's most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world's largest accommodation provider, owns no real estate"[3]. As a result, we live in an age of elapsing competitive advantages: traditional industries, established companies, and existing business models are as increasingly being disrupted. The time for a startup to reach a market capitalization of $1B, for instance, has shrunk from 20 years for

* The author would like to thank Andrea Gilli for the precious discussions and inputs provided throughout the preparation of this chapter.

[1] World Economic Forum, *White Paper Digital Transformation of Industries*:, in collaboration with Accenture, Digital Enterprise, January 2016, p. 6.

[2] M. Andreessen, "Why Software is Eating The World", *Wall Street Journal*, 20 August 2011.

[3] T. Goodwin, "The Battle is For the Customer Interface", *Techcrunch.com*, 3 March 2015.

Fortune 500 companies to 8 years for Google and three years or less for Uber, Snapchat, and Xiaomi[4].

Western military superiority is based on such a quantitative power advantage that it cannot be addressed anytime soon[5]. Thomas Mowle and David Sacko, for instance, highlight that "American military spending approaches 50 percent of the world total", and the US is "the only country that can deploy a significant portion of its military power to far-flung regions of the world"[6]. Similarly, former Undersecretary of Defense Robert O. Work notes that while at "the height of its naval dominance, England strove to achieve at least a 'two-navy standard'", currently, in "terms of aggregate warship tonnage, […] the United States enjoys a '17-navy standard'"[7]. However, this measure even underestimates real military power disparities as the United States can currently hit over 7,000 aimpoints per day in any region of the world. France comes next, with 64[8].

According to many, Western countries' technological superiority is quickly eroding because of globalization, the ICT revolution and new opportunities for industrial espionage, including cyber hacking. On the one hand, globalization is spreading arms manufacturing capabilities around the world through foreign direct investments as well as simple trade-induced transfers of technology. The emergence of dual-use components is then endowing a plurality of actors with militarily valuable capabilities, while dramatic improvements in digital and software technologies are allegedly making industrial and especially cyber-espionage much easier. As a result, so the story goes, our adversaries can mimic, with increasing ease, allies'

---

[4] World Economic Forum (2016), p. 7.

[5] N. Monteiro, *Theory of Unipolar Politics*, Cambridge, Cambridge University Press, 2014.

[6] T. Mowle and D. Sacko, *The Unipolar World An Unbalanced Future*, New York, NY, Palgrave MacMillan, 2007, p. 146.

[7] R.O. Work, *"To Take and Keep the Lead": A Naval Fleet Platform Architecture for Enduring Maritime Supremacy*, Washington, DC, Center for Defense and Budget Assessment, 2005, p. 79.

[8] Ibid., p. 96.

military platforms, as recurrent media attention toward Iran's unmanned systems, China's combat aircraft, or North Korea's plans to build nuclear-propelled submarines apparently show.

On the other hand, many argue, technological change – through so-called disruptive or emerging technologies – is challenging military superiority also indirectly. Simply put, the accelerating pace of innovation in commercial markets is increasingly endowing different actors with cheap but high-performance technologies, thus even capable of neutralizing traditional weapon systems. As a result, rivals and adversaries can compete with NATO countries and offset their force structures, at a fraction of the cost and of the time, just by exploiting some emerging technologies or capabilities.

Human Ages and Machine Ages

There is little doubt that technology has played a pivotal role in the social, economic and political developments observed over the past 200 years. This is obviously true also for international politics. The train and expansion of railways led to the end of the Colombian Era and the unification of the Eurasian landmasses[9]. The submarine and the torpedo contributed to the demise of British naval mastery[10]. The machine gun, with its radical increase in lethality, brought about a revolutionary change in land warfare – the so-called modern system of force employment[11]. Last but not least, nuclear weapons have somehow reified the bipolar and then unipolar structure of world politics[12]. As we

---

[9] B. Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony", *International Security*, vol. 28, no. 1, Summer 2003, p. 9.

[10] P.M. Kennedy, *The Rise and Fall of British Naval Mastery*, New York, NY, Humanity Books, 1976.

[11] S.D. Biddle, *Military Power: Explaining Victory and Defeat in Warfare*, Princeton, NJ, Princeton University Press, 2004.

[12] K. Waltz, "The Spread of Nuclear Weapons: More May Better", *Adelphi Papers*, no. 171, London, International Institute for Strategic Studies, 1981; R. Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*, Ithaca,

are entering a new Age in human history, the Information or Cognitive Age, and even more, looking further to the so-called Imagination Age[13], and new revolutionary technologies are being deployed, the question is whether and what effects they will exert on international affairs and global security.

Humankind has moved through, and has in front of itself, several significant stages of development. We can point out four distinct different moments, looking from the far past to the deep future, which have an interlinked existence with the evolutions of machines:

1. Agricultural Age (8,000 BC - circa 1750) The economy of this Age revolves about physical work, aided by tools that were born out of ingenuity and "technological" thinking, actively built by humans from scratch and not (only) modifying pre-existing structures. Humans are using natural energy to satisfy their needs.
2. Industrial Age (circa 1750 - 1950) The economy extensively re-organizes for the purpose of manufacturing, moving from artisanal to mass production. It is centered on factories producing commodities. Humans are substituting natural power with machine power.
3. Information Age (circa 1950 - 2050) Economy is dominated by knowledge workers using computer and other electronic devices in sectors like research, finance, consulting, information technology, and other services. Products are not physical anymore, and machine power is now substituting information and goods.
4. Imagination Age (circa 2050 – 2100)[14] We see

NY, Cornell University Press, 1989; N. Monteiro (2004).

[13] R.J. King, *The Emergence of a New Global Culture in the Imagination Age*. British Council, 2007; R.J. King, *Our Vision for Sustainable Culture in the Imagination Age*, The Imagination Age, 2008.

[14] If the exponential progression exhibits a persistent nature throughout time, the end of Imagination Age might come at that date or even earlier. 2100 is also assessed as a pivotal point for humanity by the analysis carried out by the Club of Rome and MIT in the early 1970s. See D.H. Meadows, D.L. Meadows, J. Randers, and W.W. Beherens III, *The Limits to Growth. A Report for the Club of Rome's Project*

> developing an economy where intuitive and creative thinking is the primary creator of economic value, after logical and rational thinking has been outsourced to other economies. The value is in innovating and pushing intellectual, imaginative, and creative boundaries, when information and knowledge are boundless and at anyone's disposal. Products are not just digital: they are of a hybrid nature blending digital, information, knowledge and physical worlds.

We described only these four Human Ages above because they are the only tightly interlinked with Machine Ages, namely paradigms accompanying the radical changes in employment of machines alongside the shifts in human evolutions. We understand Machine Ages as enablers and drivers for a change from a Human Age to the following one. We can identify then three Machine Ages, one per each of the transitions across the four Ages above.

1. First Machine Age: enabler of the shift from Agricultural Age to Industrial Age. The first machine age was, fundamentally, about substituting natural energy (humans, animals, water, and wind) with machine power for the production of physical goods15.
2. Second Machine Age: enabler for the evolution from Industrial Age to Information, or Cognitive, Age. This is where we are at present, and its effects are just beginning to unfold. The second machine age represents a vital breakthrough from the Agricultural model as it is centered on the digitalization of information, and thus on the production of mostly digital goods[16]. The explosion of Artificial Intelligence in this age – that from a

---

on the Predicament of Mankind. Universe Books, 1972.

[15] C. Freeman and F. Louçã, *As Time Goes By From the Industrial Revolution to the Information Revolution,* Oxford, Oxford University Press, 2001.

[16] C. Shapiro and H.R. Varian, *Information Rules: A Strategic Guide to the Network Economy,* Cambridge, MA, Harvard Business School Press, 1999.

strategic point of view can be regarded as the digitalization, demonetization, dematerialization, democratization of intelligence, and thus marking the beginning of the exponential tail[17] for intelligence – gives rise to AI-assisted tools and AI-made tools for humans.

3. Third Machine Age: enabler for the transformation from Information, or Cognitive, Age to Imagination Age. The third machine age will probably mark a transition from the creation of digital goods and information from machines, for the use of humans, to the creation of knowledge and expansion to other machines. In this sense, as also outlined as a characteristic of the Imagination Age, the goods will be of a hybrid nature blending digital, information, knowledge and physical worlds, having machines by machines and machines for machines, with AI-conceived tools for the use by other machines and AI-recombined knowledge to be consumed by humans.

As humankind navigates in the Information, or Cognitive, Age pushed irresistibly by the drivers of the Second Machine Age, and sets sail towards the Imagination Age as the Third Machine Age will develop, new revolutionary technologies are being and will, even more, be deployed. Our question is whether and what effects they will exert on international affairs and global security. In order to answer this question, we illustrate the forces that are and might keep shaping the futures, discuss the impact on future Armed Forces, and finally we describe the most immediate implications for Defense Science & Technology.

Three Shaping Forces

Three main forces are likely going to affect the production and employment of military power: convergence, complexity, and

[17] See "Exponentiality" later in this chapter.

exponentiality. Convergence relates to the increasingly intertwined nature of technological progress. Progress in software enables developments in chemistry that, in turn, permit improvements in biology, leading a cascade effect. New disciplines born in the last 15 years, like bioinformatics or quantum chemistry are a perfect example of convergence in action. Complexity reflects the impossibility to capture the entirety of interactions and their inextricable nature. Since in a complex scenario we cannot reduce the difficulty of the problem by studying the parts to understand the whole, new ways of framing the problem are needed in complex environments. Exponentiality refers to the exponential growth of technology and its effects. One of the most important is an exponential "compression" of time, as time has exponentially more value than before as a resource to achieve the desired endstate.

Convergence

Among the paramount evolutionary forces there is the confluence of future trends and themes[18], called Convergence. This refers to the interactions and intersections of different trends, resulting in a force multiplier for their effects, bringing an explosion of technological innovation. The Convergence is chiefly driven by the rate of technological advancement affecting almost every theme from political, human, and socio-economic to environmental. Interconnectedness will open up the potential for more interactions between trends resulting in a boost in technological innovation. An increased rate of advancement in individual technologies will lead to new technologies and novel usage that will have seismic, disruptive impacts. The exponential growth of technology brings, in turn, an exponential "compression" of time, as time has exponentially more value than before as a resource to achieve the desired endstate. We

[18] A theme is a collection of trends of the same epistemological nature. A usual way of clustering is through taxonomies of the transactional environment, such as PEST or STEEP.

are "in the second half of the chessboard"[19] and any delay could amount to an insurmountable chasm.

Complexity

The world is transforming at an exponential, and sometimes over-exponential, pace in multiple and deeply interconnected areas. The ever-growing number of stakeholders involved in a scenario, combined with interconnection, booming change, and confluence of technological or socio-technological trends, represents a paradigm shift from a complicated to a complex environment. Whereas in a complicated environment the analysis of interactions among many actors can still deliver reasonable conclusions able to support decision-making, in a complex environment there are simply too many interactions to be understood in their entirety, increasing the risk of surprise or strategic shock. Decision-makers will be challenged with even broader and more complex challenges when trying to achieve unity of action among many parties, to the point of being unable to define success or failure, victory or defeat. The complexity will also enlarge the number of possible trajectories pointing at desired endstate. This will, in turn, require for the leadership to embrace and master a decision-making paradigm more comprehensive, flexible, and adaptive, both at geostrategic level and within the Nations.

Exponentiality

Exponentiality is an effect and a cause for the Convergence and complexity to happen and thrive. This is the characteristic of many trends, mainly underpinned by technology, of multiplying by a constant factor a certain measure of their effects, over a limited amount of time. While the epitome of this trait is found in the evolution of computing power, known as Moore's Law, it is not a monopoly of that field. Connectivity (in terms

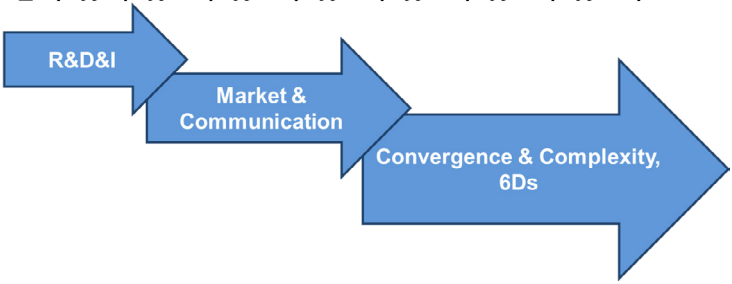
[19] R. Kurzweil, *The Age of Spiritual Machines: When Computers Exceed Human Intelligence*, Penguin, 1999, p. 37.

of bandwidth)[20], volume of data[21], and company value (retrospectively) for the so-called Unicorns, start-ups with a market valuation of more than $1B, are all exponential.

Imagining to decompose formally this exponential trend in its polynomial factors, à la Taylor, we can appreciate the existence of macro-clusters pointing at a deeper structure emerging underneath the exponential drive for trends.

Fig. 2.1 - Exponential decomposition of trends *à la* Taylor

$$e^x = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + \cdots$$



The lower-degree push is given by research, development, and innovation, which we can see as "first movers" for trends[22]. The medium-range can be seen as covered by public acceptance, strategic communication, and investment. The higher-degree factors cover the "exponential tail" of the decomposition, leading to the effects of the Convergence. In this sense, some descriptive qualities from Diamandis' 6Ds, namely digitalization, demonetization, dematerialization, democratization[23], can be

[20] CISCO, *CISCO Visual Networking Index: Forecast and Trends, 2017-2022*, CISCO White Paper, 2018.

[21] Ibid.

[22] Scientific knowledge creation is at most quadratic. Analysis of the data from arXiv, 1991-2019. See also G. Rizzo, *Convergence, Complexity and Exponentiality: irresistible forces, irreconcilable antagonists*. Anticipation-Agency-Complexity International Workshop, 2017.

[23] P.H. Diamandis and S. Kotler, *Bold*, New York, NY, Simon & Shuster, 2015, p. 16.

used as a key to having some hints on the content belonging to this tail.

Such a decomposition can be an enabler to seize the initiative when an innovation is still in the realm of weak signals and barely surfacing among the noise and, conversely, a way to force trends of pivotal interest for Defense, which might be still lying in the linear regime, up in the exponential curve. It is becoming harder and harder for the Defense complex to maintain the technological edge and the scientific advantage on the commercial market and other competitors exploiting "grey" techniques, and this decomposition can provide a supporting key to interpret evolution and changes in the technology landscape at its largest.

Not all trends are "just" exponential. Whenever two exponential trends are merging under the force of Convergence, depending on some "fundamentality" characteristics[24], they produce over-exponential effects. Examples for this kind of uber-trends are rare at the moment but a) nevertheless existent and b) will likely see significant and unexpected growth in the next ten years due to the Convergence's "selective pressure" towards exponentiality. The first example (by Alexander Kott at US Army Research Laboratory) is weapons capability[25], which is evolving at a quadratic-exponential pace[26]. Namely, what Kott finds is that a composite measure of an artifact's attributes (called Figure of Regularity) for mobile direct-fire systems grows over a span of seven centuries with this rate. He examines such factors as the year of the weapon's creation, the velocity of the projectile it fires, the mass of the projectile and of the weapon itself, how fast the weapon moves, the rate of fire, crew

[24] A. Gilli and G. Rizzo, work in progress. See also "Recombination of Innovations" later in this chapter.

[25] A. Kott, "Toward Universal Laws of Technology Evolution: Modeling Multi-Century Advances in Mobile Direct-Fire Systems", *Journal of Defense Modelling & Simulation*, preprint.

[26] This means that, broadly, the effect is not just multiplied every certain amount of time, but the very factor it is multiplied by is doubled every time.

size, and so on. All these aspects are placed in a formula to show how one innovation sets the stage for another one. Based on his work, Kott believes that advancements in technology, or a complex of technologies, (e.g. soldier-worn exoskeletons) will enable dismounted troops to carry a good deal more armor and firepower as, given current trajectories, they should increase soldier carrying capacity by 50 percent by 2050[27].

The second example is quantum computing power, which apparently has the potential to evolve at a double-exponential pace[28]. Quantum computing power depends on a characteristic called "dimension of Hilbert space". Over the next fifty years, if we assume a type of Moore's law for quantum processors with the number of qubits in the processor following an exponential growth doubling in size every few years, since the dimension of the Hilbert space scales exponentially again with the number of qubits, the computing power will scale double-exponentially.

---

[27] Based on that, and the long-term trends of evolution of firearms in terms of speed of fire and the kinetic energy they deliver per projectile, he anticipates that future foot soldiers in their battery-powered armor suits might rock machine gun that are today usually mounted on vehicles or tripods, guns like the Chinese QJZ-89 and the Russian Kord. Tanks, too, will get heavier and better-armed. Current trends suggest that tank units of 2050 might boast 70-ton tanks crewed by three or four people and armed with a 152mm or even 155mm gun, similar to an M777 howitzer. But Kott also foresees smaller, two-person tanks that can move offroad at 45 km/h, putting up to ten 135mm rounds a minute on targets out to 5,000 meters.

[28] H. Neven, at Google Quantum Spring Symposium, May 2019.
That is very fast. Looking at Moore's Law, it is perfectly reasonable to assume an increase of 3 orders of magnitude every 20 years. Starting then with 1 qubit in 2000 (and Hilbert space dimension of 21, which is 2), the first step is some system that may have 1000 entangled qubits in 2020 with a Hilbert space dimension of 21000 or 10300. The third leap (2040) might have 1,000,000 entangled qubits or a Hilbert space of 21000000, that is about 10300000. In 2080 we might have algorithms running on a trillion-qubit machine (of unknown technology) that has a Hilbert space dimension of 2100000000000 or 10300000000000. This implies that we will cover 300,000,000,000 orders of magnitude of Hilbert space in the next fifty years compared to 60 orders of magnitude covered in the past several thousand years. In this sense, the perspective technological evolution incoming in this century might be unrivaled in the history of human species.

Here the effect is diverging very fast[29], to reach a point where the perspective technological evolution incoming in this century might be unrivaled in the history of human species. The introduction to this chapter is indeed just a consequence of exponentiality and convergence.

Shaping Forces and Machine Ages

Complexity, convergence, and exponentiality are drivers for the evolution of Machine Age, which, in turn, are forcing Human Ages to shift. This is clear in the second machine age, which represents a major breakthrough from the Agricultural model as it is centered on the digitalization of information and thus on the production of mostly digital goods[30]. This transformation is the result of the interaction among three main dynamics[31]. First, exponentiality: Moore's Law. The power of processors has dramatically expanded over the past forty years; the number of transistors that can fit on a silicon chip has, in fact, systematically doubled every two years starting from 1971, enabling the production of increasingly powerful but also smaller devices[32]. For instance, the computing power of any smartphone or a WiFi router is more than that of the MIT-produced command module computer that assisted NASA's Apollo mission[33].

---

[29] To put exponential and these other two kinds of over-exponential in scope, the growth of the exponential trend is multiplied by 2, 2, 2, 2, 2, 2, and so on. The multiplying factor stays the same. In the quadratic-exponential trend, the effect is multiplied by 2, 4, 16, 96, and then approximately 750, 8000, and 95000 in the same time span. And for the double exponential we have 2, 4, 16, 128, and then approximately 2000, 65000, and 2,100,000.

[30] C.Shapiro and H.R. Varian, *Information Rules: A Strategic Guide to the Network Economy,* Cambridge, MA, Harvard Business School Press, 1999.

[31] E. Brynjolfsson and A. McAfee, *The Second Machine Age*, 2014.

[32] M. Lundstrom, "Moore's Law Forever?", *Science*, vol. 299, no. 5604, 2003, pp. 210-211.

[33] With 64Kbyte of memory and operating at 0.043MHz, the AGC's performance simply pales in comparison of an iPhone 6: through an Apple-designed 64 bit Cortex A8 ARM architecture composed of approximately 1.6 billion

Second, complexity: software capabilities have increased by a degree of magnitude since the birth of computers. Third, convergence: machines are not just substituting physical power, but digital power and the goods in that sphere.

The transformation brought about by the second machine age is having and will have disruptive implications for the economy, society, and politics. For instance, according to the consulting company McKinsey & Co, some $16 tn wages are currently paid for activities that could be soon automated[34]. Similarly, given what we have seen over the past decade, entire industries will be turned upside down[35]. "Uber, the world's largest taxi company, owns no vehicles. Facebook, the world's most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world's largest accommodation provider, owns no real estate."[36] Corporations will have to go through profound transformations in order to better exploit data analytics. The opportunities for business are enormous. For example, in offshore oil rigs, "less than 1 percent of the data generated by the 30,000 onsite sensors" are currently used to inform decisions[37]. This could generate billions in savings around the world. However, such business reorganizations will be neither easy nor quick: data analytics, for instance, will have to be moved from IT departments to operations, but as artificial intelligence progresses further, the rationale for automating strategic decisions will strengthen further[38].

---

transistors and operating at 1.4 GHZ, it can 3.36 billion instructions per second.

[34] J. Manyika, M. Chui, and M. Miremadi, *A Future that Works: Automation, Employment and Productivity*, San Francisco, CA, McKinsey Global Institute, 2017, p. 8.

[35] A. Ross, *Industries of the Future*, New York, NY, Simon & Schuster, 2016.

[36] T. Goodwin, "The Battle is For the Customer Interface", *Techcrunch*.com, March 3 2015.

[37] James Manyija et al., *The Internet of Things: Mapping the Value Beyond the Hype*, San Francisco, CA: McKinsey Global Institute, 2015), p. 4.

[38] T.H. Davenport, "Rise of the Strategy Machines: While humans may be ahead of computers in the ability to create strategy today, we shouldn't be complacent about our dominance", *Sloan Management Review* 58, no. 1, Fall 2016.

This wave of technological change is increasingly opening new opportunities. As Erik Brynjolfsson and Andrew McAfee note, however, we are just entering the second machine age[39]. Most of its wonders have thus still to come[40].

Recombination of Innovations

Complexity and convergence show their action in the recombination of innovation and their transferability to other fields, even non-adjacent. One famous example is Transfer Learning, a general property of trained AI networks that allows a "trained AI" to be used for another, different, task and still be able to use the knowledge gained in the first field. More in detail, Transfer Learning is a research problem in machine cognition that entails storing knowledge gained while solving one problem and applying it to a different one[41]. A second one is a recent report on how Liverpool FC employed missile-tracking electro-optics technology and data science to recruit players and uses mathematical models to select its manager[42].

In the Defense field, seapower and underwater warfare are valid examples. Sound represents the primary way of detection. For this reason, navies have been investing increasing resources for the past decades in quieting techniques and technologies. More powerful sensors, thanks for sustained growth in software and hardware capabilities, promise to increase precision and detail of identification and tracking, to the point of having a "Transparent Ocean" ultimately dramatically revolutionize underwater warfare and strategic triads. Robotics, and more precisely the possibility to distribute capable sensors and

---

[39] Erik Brynjolfsson and Andrew McAfee, *The Second Machine Age*.

[40] A. Ross, *Industries of the Future*, New York, NY, Simon & Schuster, 2016.

[41] L. Pratt, "Special Issue: Reuse of Neural Networks through Transfer", *Connection Science*, vol. 8, no. 2, 1993.

[42] J. Burt, "How Liverpool employ missile-tracking technology to recruit players and used a mathematical model to hire Jurgen Klopp", *The Telegraph*, 11 November 2019.

processors, is further strengthening this dynamic. The logic is straightforward. Because of the laws of physics, long-range detection depends on the size of the radar antenna or of the sonar dome. Larger radars or sonars require however bigger platforms that, as such, are inherently easier to detect and thus require either more capable defense systems (in the case of warships) or significant investments to reduce sound propagation (submarines). By distributing smaller and autonomous surface and underwater platforms, navies can extend their perimeter of operations; oceanic surveillance is a good example.

What Problem for Future Forces

To keep the military edge and prevail in future operations, armed forces must continually evolve, adapt, and innovate.

If forces can keep the military edge, the West "at large" in its ontological sense will have the advantage over potential adversaries. Keeping the edge means it has to be proactive and have the best human capital, technology, education, and training. Prevailing in future operations means that Forces will able to accomplish their assigned missions and affect the will of the adversary through a combination of interdomain effects. Through critical thinking, continual evolution, adaptation, and innovation, they will learn and grow to conduct future operations more efficiently and effectively. To achieve this central idea, forces will need to be credible, networked, aware, agile, and resilient[43].

Nowadays, technological giants (or, as Gartner calls them, Digital Dragons)[44] like Google, Apple, and Amazon have outpaced all other corporations in terms of profits, income and

[43] NATO, *Strategic Foresight Analysis*, 2017; NATO, *Framework for Future Alliance Operations*, 2018.

[44] S. Moore, "How to Become a Digital Dragon", *Smarter with Gartner*, Gartner, 2017; L. McMullen and D. Aron, *Winning in a World of Digital Dragons*, Gartner, 2018.

market capitalization[45]. The critical question is whether the companies of the new economy will represent the backbone of American military-technological superiority also in the decades ahead. The former US Secretary of Defense, Ashton Carter, seems support this view. In fact, he has launched a *Third Offset Strategy* aimed at promoting the development and integration of new radical technologies in the US military and, for this purpose, he has even opened a Department of Defense innovation unit (DIUX) in the Silicon Valley[46].

These dynamics have extremely important implications, not only for policy-makers but also for international relations theory and European security more in general. Technological change affects industrial hierarchies and, ultimately, when it comes to military systems, the global distribution of power[47]. Technological change can, in fact, further reinforce leading players (competence-enhancing or evolutionary innovations), or it can favor the rise of new companies and hence reshape the existing international order (competence-destructing or revolutionary innovations)[48]. The application of gunpowder

---

[45] "FT500: The world's largest companies", *Financial Times*, 31 March 2016.

[46] R. Martinage, *Toward a New Offset Strategy: Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Project Capability*, Washington, DC, Center for Strategic and Budgetary Assessment, 2014; N. Syeed, "Can the Pentagon Learn to Be Flexible? A Defense program tries to partner with tech companies", *Bloomberg*, 9 June 2016.

[47] Ja.Utterback and F.F. Suarez, "Innovation, Competition, and Industry Structure", *Research Policy*, vol. 22, no. 1, 1993, pp. 1-21; C.M. Christensen, F.F. Suárez and J.M. Utterback, "Strategies for Survival in Fast- Changing Industries", *Management Science*, vol. 44, no. 12, December 1998, pp. 207-220. For a discussion of the consequences on international politics, see R. Gilpin, *War and Change in World Politics*, Cambridge, Cambridge University Press, 1981; and M.C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics*, Princeton, NJ, Princeton University Press, 2010.

[48] M.L. Tushman and P. Anderson, "Technological discontinuities and organizational environments", *Administrative Science Quarterly*, vol. 31, no. 3, September 1986, pp. 439-465; R.M. Henderson and K.B. Clark, "Architectural Innovation: The Reconfiguraion of Existing Product Technologies and the Failure of established Firms", *Administrative Studies Quarterly*, vol. 35, no. 1, 1990, pp.

to warfare, and thus the introduction of cannons epitomizes a competence-destructing innovation: it required dramatically new skills and know-how in manufacturing, which in turn led to the demise of the knighted nobility in Western Europe and thus to the emergence of centralized states. Conversely, the introduction of precision-guided munitions during the 20th century represents a competence-enhancing innovation: it built on recent technological developments based, among others, on radar, communications, and propellers, among others, and thus further widened the gap between dominant countries (the US and Western Europe) and the rest[49].

Whether the effects of the Second Machine Age will be competence-destructing or competence-enhancing is the central question of our age. Policy-makers and scholars disagree in fact as to what effect dual-use components, cyber capabilities, and more generally this technological revolution will have on US and Allied military-technological superiority[50].

Technological change is on a strong exponential track, with a consistent record over the last few decades. If this reveals to be a foundational characteristic of this era and this century in particular, contrary to the "common sense" intuitive linear growth, we will not experience 100 years of progress in the 21st century – it will be more like 20,000 years of progress[51].

9-30; P. Anderson and M.L. Tushman. "Technological Discontinuities and Dominant Designs: A Cyclical Model of Technological Change", *Administrative Science Quarterly*, vol. 35, no. 4, December 1990, pp. 604-33; R. Henderson, "Underinvestment and Incompetence as Responses to Radical Innovation: Evidence from the Photolithographic Alignment Equipment Industry", *The RAND Journal of Economics*, vol. 24, no. 2, Summer 1993, pp. 248-270.

[49] R.O. Work, *To Take and Keep the Lead: A Naval Fleet Platform Architecture for Enduring Maritime Supremacy*, Washington, DC, Center for Strategic and Budgetary Assessment, 2005; B.D. Watts, *The Evolution of Precision Strike*, Washington, DC, Center for Strategic and Budgetary Assessments, 2013.

[50] Technological revolution is also just an enabler among more enduring characteristics of US military-technological superiority. See L. Colucci and G. Rizzo, *A Grand Strategy for the Long Peace*, work in progress.

[51] R. Kurzweil, *The law of accelerating returns*, Kurzweil Essays, 2001.

Taking this trend as persistent and not transitional in the transactional environment, its consequences are mostly beyond imagination. The ones we can grasp, however, are huge. With this assumption, in the horizon 2040-2050 (during the Third Machine Age and entirely moving into Imagination Age), we are going to see developing a "hyper" tier of conflict – hyperbolic, hypersonic, hypercontested.

Hyperbolic warfare, or hyperwar, is AI-fueled, machine-waged conflict[52]. What makes this new form of warfare unique is the unparalleled speed enabled by automating decision making, and the concurrency of action that becomes possible by leveraging artificial intelligence and machine cognition. In military terms, hyperwar may be redefined as a type of conflict where human decision making is almost entirely absent from the observe-orient-decide-act (OODA) loop. As a consequence, the time associated with an OODA cycle will be reduced to near-instantaneous responses. The implications of these developments are many and game-changing, like infinite, distributed Command & Control capacity, concurrency of action and perfect coordination, logistical simplification and instant mission adaptation. In hyperwar, the situation we might be facing is that of an opponent being able to decapitate or destroy Blue forces completely before Blue being able even to make a decision. In this sense, this is not just a "Digital Dreadnought" keeping adversary off-balance, but an entire shift in the application of forces. Hyperwar is beyond total war: in hyperbolic warfare technology is completely oriented to generate destruction[53].

Hypersonic means not just the employment of assets and kinetic effectors at speed greater than Mach 5, but also the overall posture of embracing and exploiting the compression of time. Directed energy weapons also "lie" in this label, despite being speed-of-light – much more than hypersonic.

---

[52] J.R. Allen and A. Husain, *On Hyperwar*, US Naval Institute, July 2017, vol. 143, no. 7, p. 1,373.

[53] G. Rizzo (2019).

Hypercompetition, or the condition causing the strategic space to be hypercontested, describes conditions where competitive advantage is not sustainable and/or competitors are persistently attempting to erode the opponent's competitive advantage[54]. The hypercompetitive military rivalry is a persistent struggle for important but transient advantage across and within highly contested spaces – air, land, sea, space, and cyber domains; the electromagnetic spectrum, and the strategic influence space. Contemporary hypercompetition requires constant layered competitive activity across and within what are highly-contested strategic spaces. Hypercompetitive advantage most often goes to rivals that are biased for action and postured to seize transient opportunities[55].

We identify six topics of utmost importance for future Armed Forces and Military Instrument of Power from the Second to Third Machine Age. The tenet future Military Instrument of Power will likely be called to adhere to could be phrased as "instant decision, perfect action".

Understand and anticipate complex behavioral dynamics

The multiplication of possible trajectories connecting a given status quo to the desired endstate[56] is among the consequences of the Complexity-Exponentiality-Convergence triad. Due to the rapid expansion of the space of possible decisions, the role of exploring not even all of them, but also just a majority, is a task which cannot be carried out by humans alone. Being able to simulate in-depth the broad range of dynamics – happening strategically at the intersection of diverse paradigms of value, ethics, operational needs, societal context and policy, or

[54] R.A. D'Aveni, *Hypercompetition – Managing the Dynamics of Strategic Maneuvering*, The Free Press, 1994.

[55] N. Freier, *Game On: Hypercompetition and Advantage in the PACOM AoR*, US Army War College, 2018.

[56] We actually hypothesize that the set of trajectories from the present to a given endstate is dense (in the set theory sense of the term) in the cone of futures.

operationally at the intersection of tactical conditions, mission priorities, culture, local context, previous history – could shorten the decision cycle significantly, presenting a fuller assessment and a more complete overall picture. Leveraging big data "in the back-office", with their staff, to augment the analysis process, enrich its structure, broaden its depth, to solve the confusion and the uncertainty brought by too much information, too much interlinked, the leadership will be enabled in delivering better decisions, faster.

Guarantee awareness and jointness[57]

Situational awareness and unity of action will be even more crucial in high-intensity, high-tempo operations against near-peers in multi-domain, multi-speed Theaters with possibly hard denial[58] of some kind. Sensors will need to scale beyond limits imposed by the way we conceptualize sensing, and communications might need to be radically evolved to happen in a different way so as to escape any possible blockade. At the same time, the exponential acceleration required to responses will put the jointness of the Armed Forces and the unity of action of the Military Instrument of Power at risk of disruption, due to the mosaicked nature of the future threat landscape[59] and the pressure to act with decision-action cycles shrunk to zero time. These two factors combined have the potential for a disruptive disconnect between the strategic and the operational level, and even within and across the latter.

---

[57] Jointness implies cross-Service combination wherein the capability of the joint force is understood to be synergistic, with the sum greater than its parts (the capability of individual components).

[58] Hard denial could happen not just in electromagnetic space, but in physical space as well, and not in terms of "classical" domain superiority. For instance, if either through technological advances, or due to a radical change of climate conditions, or both, could be possible to trigger a phase transition of the atmosphere into a turbulent regime, the air domain would be effectively denied not through adversarial control.

[59] T. Grayson, *Mosaic Warfare*. DARPA; 2018; T. Hitchens, *DARPA's Mosaic Warfare - Multi Domain Ops, But Faster*, Breaking Defense, 10 September 2019.

Leverage the increased complexity of the environment

Future forces will need to operate in increasingly complex environments, at all levels in the spectrum of conflict. They might also have to confront organizations culturally far, or with an ethical or moral background we do not entirely understand. This could result, on the one hand, in competing against organizations or actors with structures and processes we do not conceive, and on the other hand in an impossibility to support decisions through old-style human reasoning. Being able to employ game-changing capacities to understand exponentially more complex scenarios means having the ability to have double-exponentially more powerful capacity: a first exponential for the shift from complicated to complex and a second for the acceleration in complexity. Forces and the Military Instrument of Power as a whole will need not just to be able to prepare, withstand, recover and respond to threats and shocks, but even benefit from them – as shocks will be coming as "the new normal". Being able to show this characteristic would amount to proving an incredibly powerful passive deterrent.

Respond, escalate, de-escalate with agility, flexibility, and incisiveness

The future geostrategic and operational environment is on a track to be in the "hyper" tier – hyperbolic, hypersonic, hypercontested. Strategic and operational responses will need to be fast, timely, and supported by extremely flexible decision-making able to understand hypercompetition and seize hypercompetitive advantage. Future adversaries and actors might want to move into this very area to keep us off-balance, confronting us extensively in hypercompetition, trying to escalate infinitely fast exploiting the hyperbolic character of war and then de-escalating equally fast, looking again for dialogue, trying to exploit the ontological stance of the West at large of being "the good guys" and thus never turning down an opportunity for dialogue and de-escalation. These immensely fast changes in

the environment at all levels of the spectrum, from strategic to operational to tactical, will require to exploit deeply the best of both worlds provided for by the Third Machine Age – agents, assistants, advisors from the artificial world and creativity, empathy, ethics from the biological world.

Leverage infinite bandwidth, infinite data, infinite access

The exponential growth of technologies and their subsequent effect on total available bandwidth and data will create the conditions to have almost infinite quantities of these two resources – a situation never happened before in the history of humankind, as there has never been a time when resources had not been limited and contested, in a way or the other. It is interesting to note how this reversion of perspective has been possible thanks to the digitization, democratization, and dematerialization of these resources[60]. Being able to govern and direct the abundance thus available will be a challenge of which the future Forces will be part of. At the same time, they will face a more pragmatic situation: how to operationalize this abundance to create strategic advantage and seize or maintain the initiative in higher and higher tempo operations. Future Forces and Military Instruments of Power will need to be able to understand and exploit the thin boundary between cyberspace and physical space – the so-called cyber-physical space – where bandwidth, data, and access flow into physical characteristics to become actionable elements of the strategic environment. As such, there might be the need of re-thinking the way of interacting with machine and the cyber world, to capture this precious essence existing in none of the two worlds separately, but just in that realm of contact with one another (the boundary, in fact).

[60] See section "Exponentiality", earlier in this chapter.

Create surprise

Future Forces will be depending even more on fundamental and groundbreaking research. Research and engineering are done for three reasons. The first is to mitigate current threats, and very soon, future threats. So that involves electronic warfare, cyber defense, maintain space capabilities, counter WMD, and missile defense. Those are capabilities that are making up the fundamentals of our defense and are still going to be relevant.

The second reason to do research and engineering is to build affordability into the assets being procured. That talks about doing better systems engineering upfront, enhancing modeling and simulation capability, open systems architectures, prototyping to retire technical risk. So the second reason is more affordability, but it is attacked not through technology areas but through processing.

The third reason to invest in research and engineering or Science and Technology is to build technology surprise, to reach a point where we have a way to put our adversary permanently off-balance without possibility of recovery. Technology surprise is an enabler of univocal and unbalanced advantage and has thus to be continuously pursued.

How To Maintain Superiority

Military superiority is also maintained through a long-term, extensive and systemic strategy for technological advantage, aiming at preserving the Offset, "a persistent, pervasive, univocal and unbalanced advantage, which shifts the competition from an unfavorable scenario to one that allows the application of forces to an otherwise immovable problem, or surmountable at an unacceptable cost. The Offset is at the heart of strategic advantage, and is generally achieved through a long-term technological superiority strategy (*offset strategy*)"[61]. Offset strategies,

[61] D. Panebianco, G. Rizzo, M. Ruggieri, E. Trenta and Gabinetto del Ministro

then, are the actionable engagement resulting from foresight and scoping deep futures – and the three taken together are our only way to weaponize the future. An essential step here is understanding the nature of technologies and their effects both in the technological space and in the broader picture of the Defense space and the future Armed Forces, to try and anticipate the most relevant interactions, possibly driving or resisting the Offset strategy. Good technology is a function of good strategy, and it pays dividends[62]. This is well known in history and especially in US strategy over the past decades.

First, during the 1950s, President Dwight Eisenhower's "New Look" strategy built up America's nuclear deterrent as a means of countering the Soviet Union's conventional superiority in Europe – nuclear weapons, long-range bomber forces, and missile forces: the first example of a total orientation of technology towards long-term victory. At the time, US nuclear primacy over the Soviet Union was indisputable, which President Eisenhower exploited. Even after US nuclear primacy began fading, starting in the 1960s, and despite the best efforts of successive presidents, the US continued to rely heavily on nuclear weapons to offset the Soviet Union's conventional superiority in Europe.

Starting in the 1970s, however, under Defense Secretary Harold Brown and Deputy Defense Secretary William Perry, the US military began investing in new capabilities that would lead to its second offset strategy. Specifically, they began investing in extended-range precision-guided munitions, stealth aircraft, and new intelligence, surveillance, and reconnaissance platforms. These investments would continue during the Reagan administration and began coming to fruition in the 1980s in time for the First Gulf War. These investments have also anchored America's military superiority during the post-Cold War era.

---

della Difesa, *Duplice uso e Resilienza: documento di integrazione concettuale delle Linee Programmatiche del Dicastero (Dual use and Resilience: concept addendum to Programmatic Lines of Development of the Ministry)*, Ministero della Difesa, 2018, A-6.

[62] J. Lindley-French, private communication.

In 2014, Defense Secretary Chuck Hagel announced the Pentagon's new "Defense Innovation Initiative". In Hagel's words: "This new initiative is an ambitious department-wide effort to identify and invest in innovative ways to sustain and advance America's military dominance for the 21st century. It will put new resources behind innovation, but also account for today's fiscal realities – by focusing on investments that will sharpen our military edge even as we contend with fewer resources." The technological fields of interest in this Third Offset Strategy will be robotics, autonomous systems, miniaturization, big data, and advanced manufacturing, including 3D printing.

However, which technologies, or even paradigms, should we look at to obtain, consolidate and keep superiority? In the previous section, we outlined a set of problems future Forces will have to face if trends we see today will persist or even reinforce. A Fourth Offset Strategy then will have to be broad enough and specific enough to capture these issues in its aperture: we list below eight key aspects, broken down in four game-changing technology fields (Quantum 4.0, Convergent Biology, Femtotechnology, and Algebraic Ethics) and four transformational paradigms (Centaurs, Body-as-a-Node, Energetically Neutral Forces, and Antifragility).

Quantum 4.0

Listing Quantum 1.0 as quantum mechanics, Quantum 2.0 as exploiting quantum mechanical properties other than entanglement (and thus mainly quantum sensing), Quantum 3.0 as the operationalization of quantum correlations (so quantum computing, as an example), Quantum 4.0 encompasses the "more quantum than quantum". We have three vistas here. The first and bolder is on superquantum correlations[63]: being able

[63] So-called PR-boxes (from Popescu and Rohrlich). Quantum nonlocality refers to the phenomenon by which measurements made at a microscopic level contradict a collection of notions that are intuitively true in classical mechanics. Having PR boxes would mean being able to communicate in a totally uninterceptable way arbitrarily long messages with just one bit of content, provided you have

to master this new and untouched aspect at the convergence between mathematics and physics, would open the door to instantaneous[64], faster-than-light, non-interceptable communications. While of little value imagining operation at a global scale, think more broadly. Think space operations in cis-lunar region or Lagrangian points. The value of this technology amplifies with distances – the further the distance to communicate to, the more strategic advantage it provides. Moreover, since it happens in a space other than physical space, there is no way this can be degraded, disrupted, or denied.

The second is weak values amplification and the concept of weak measurements: in quantum mechanics, every measure "destroys" part of the quantum state, which is one of the two pillars rendering quantum key distribution (QKD) unbreakable. The other one is the so-called "no-cloning theorem", stating basically that quantum states cannot be copied as we do with digital data. Being able to measure a quantum state "just enough", so not extracting all the information from it but at the same time not to making it collapse, would pave the way to new and even more disruptive uses of quantum capabilities in sensing, and could also provide enough grounds to overcome, at least partly, the no-cloning theorem – so QKD might not be as unbreakable as it might seem now.

---

exp(length) PR boxes available. PR boxes are "non-signaling oracles" which are not realized in classical quantum mechanics (QM) as they are "more nonlocal than quantum nonlocality" (they have the maximal Clauser-Horne-Shimony-Holt inequality value of 4 instead of the classical QM $2+\sqrt{2} \approx 3.41$ – to be nonlocal a theory have to be this value larger than 3). See also D. Panebianco, G. Rizzo, M. Ruggieri, E. Trenta and Gabinetto del Ministro della Difesa…, cit.

[64] This would exploit what Einstein's called "spooky action at a distance". Quantum physics tells us it is instantaneous and the latest esteems look like it is right, propagating at least 10,000 faster than light. See J. Yin, et al., 'Bounding the speed of 'spooky action at a distance'", *Physical Review Letters*, vol. 110, no. 260407, 2013. This was not an actual "measurement", and it does not rule out the possibility it is instantaneous, in the sense that the effect was so fast the best measure scientists could get was bounded just by measurement errors.

The third aspect is quantum Internet and quantum high-performance clusters. To run simulations of the degree of complexity to understand and anticipate complex behavioral dynamics (as described in the previous section) we will plausibly need not a classical supercomputer, and not even just one quantum computer, but a way to do distributed quantum computing – i.e. a quantum internet. The interesting angle here is that quantum computing power scales double-exponentially in the number of qubits. So the ability to create a quantum internet, namely a way to transmit quantum information over a quantum mean, would enable the sharing of quantum information inside qubits. This means having the capacity of increasing the total number of qubits available for computation without the need of having a single huge infrastructure suited for this large compute capacity, and using them all together like they were in a single quantum computer[65] – and this results in an over-exponential speedup.

Centaurs

The exponential, and in some fields over-exponential, growth of structured and unstructured data, from human and non-human sources, marks the transition from knowledge creation being an exclusively human endeavor to its future dimension: becoming a blended, converged enterprise by Centaurs, man-machine *unicums* likening to the mythical Greek half-horse, half-man creature, blending biological and artificial intelligence into an inextricably linked, converged whole, which is more capable than the sum of its parts alone[66].

The narrative *Human vs Machine* is deeply misplaced. Intelligent machines will not replace human beings. They will fulfill some of their traditional tasks, thus opening more

[65] R. Beals, et al., *Efficient distributed quantum computing*. Proceedings of the Royal Society A, 469, 20120686, 2013, arXiv:1207.2307.

[66] G. Rizzo (2019); G. Rizzo, *Towards a Fourth Offset Strategy: maintaining the edge in hyperwar and hypercontested domains*. MILTEC19 International Conference – The Changing Face of Warfare, 2019.

space for focusing on the domains where human beings have some inherent advantages. This is why several works, including Accenture's consultants Paul Daugherty and H. James Wilson or Gen. Mick Ryan from the Australian Defense College, refer to *Human + Machine*.

In our era – the Information or Cognitive Age – data are the dispersed, ever-present dust being the invisible gold of today's markets and tomorrow's Theatres. Data do not exist just in one side of the real-virtual nexus – they are generated from events happening in either, or both, cyberspace and physical space, and their effects have ripples in all Domains of operations. As such, neither an only-physical nor a completely cyber being can capture and exploit the full potential of data. With Centaurs, the humans half brings the brain and the heart, while the machine half provides its strength, speed, and power, making sense of that data by learning and reasoning from their interactions with us instead of being explicitly programmed – making it scalable with the volume, complexity, and unpredictability of information and systems in the modern world. Both parts are inseparable, and empower reciprocally.

In the Imagination Age horizon, machines would team alongside and together with humans, potentially calling for an evolution in the nature of warfare. This already raises a flag on the horizon for a new generation of decision-making, where humans and machines are inextricably linked, bringing out the best of both worlds to the Alliance. We will likely see real machine to machine warfare, with the role of humans being fundamentally different from what it is today. The human-grade speed of decision-making might not be sufficient to keep up with the dynamics of the Theatre of tomorrow. This means that locking in just the human element in the decision-action cycle might weigh as a disadvantage for future forces. Nevertheless, it will be paramount to have a human touch as unique differentiator to raw machine power.

Convergent biology

The ability to read genomes has transformed our understanding of biology. Being able to write them would give us unprecedented control over the fabric of life. Or weave this invaluable thread and its properties into the inanimate world.

In the Fourth Offset, the aim should be at reaching full capacity in designing and constructing biological modules, biological systems, and biological machines, or re-design of existing biological systems for other purposes (the so-called "chimeras"). The artificial design and engineering of biological systems and complex living organisms for purposes of improving applications for industry or biological research, or the ability to simulate *in vivo* through "model-based bio-engineering", capturing the entirety of interaction of thousands of genomes together (of paramount relevance to anticipate effects in humans and their microbiota) would grant us ground-breaking advantage. Conversely, reaching the point of applying and interweave biological principles to nano-engineering – another glaring example of the Convergence in action – might enable us to crack machine self-replication. Write genomes from scratch and simulate their effects.

Today, rapid advances in DNA sequencing and gene-editing technology mean we are now truly in an era of genomics. For a few hundred dollars, genetic testing companies will give a detailed rundown of ancestry and susceptibility to a host of diseases. The first genetically modified humans are about to turn one. The advent of CRISPR in particular has given us the ability to modify DNA with unprecedented precision, but we are still restricted to switching specific genes on and off or swapping one gene for another. The field of synthetic biology wants to change that by bringing engineering principles to biology. Convergent biology means being able to apply principles from both, to both realms.

There are four aspects here. The first is Genome Design. The ultimate goal of genetic modification is to produce a change in the phenotype – i.e., the external characteristics – in the

target organism. However, most complex traits are the result of a complicated interaction between multiple genes and the environment, so mapping how DNA tweaks will translate into desired attributes is challenging. Large-scale genome design will require computing capabilities that can do this accurately and efficiently. While projects like Synthetic Yeast 2.0 have made the first steps in this direction, the field needs to build complex new models that can predict the results of changes to the genome sequence, and have at its disposal quantum computing capacities to get there first.

The second aspect is DNA synthesis. We have been able to synthesize DNA since 1985 with the invention of Polymerase Chain Reaction, but this is restricted to short sections of DNA just a few hundred base-pairs long. Building entire genomes requires long sequences of several thousand base pairs. Large-scale genome engineering will require much faster, cheaper, and more efficient methods for DNA assembly, designing new enzymes or, later, converging "bio" and "nano".

The third field is Genome Editing. While our gene-editing capacity has come a long way, we still struggle to make profound changes to a genome, simultaneously. If we could develop this capability, it could significantly decrease the amount of time it takes to modify organisms and build genomes from scratch. This will mean finding ways to prevent the multitude of guide RNAs (the "targeting systems" that guide CRISPR in the spot of the genome where to make changes) required for simultaneous edits to multiple genes from interfering with each other. This would also help the creation of libraries of tools for making changes across the genome and "accessibility maps" indexing how efficiently different targets can be altered.

The fourth and latest is Chromosome Construction. DNA is more than just a string of genes; it is packaged into chromosomes. We can currently just assemble and manipulate chromosomes rudimentarily. Moreover, transplanting these chromosomes into the target organism is another major bottleneck. Techniques like cell fusion and microinjection might converge

microfluidics and molecular biology. Plus a greater understanding of the fundamental infrastructure that sustains the architecture of chromosomes and how they interact.

Femtotechnology

Today we have multipurpose alloys, nano-engineered interfaces, 2-dimensional functionalized materials (graphene, silicene, phosphorene, hexagonal boron nitride – h-BN or "white graphene"). Efforts in valence band design and mechanical properties engineering starting from "prime principles", together with an atlas of microscopic structures and the resulting engineering characteristics, show that – changing a famous quote of Richard P. Feynman – "there is plenty of capacities at the bottom". What we need to aim for tomorrow, the Fourth Offset, is designing and engineering down to the single-atom scale, achieving full control at the femtometer (one-millionth of a billionth of a meter, or 10-15 m). This might not be realized just as exploiting atoms like Lego bricks, but also through macroscopic quantum phenomena (like superconductivity or giant magnetoresistance) together with other meta-engineering at the nanoscale.

Energetically neutral forces

Military capabilities of the future Forces will have to provide their energetic sustainment by integrating in the natural environment in which they are operating, so as to render the access to external sources down to null[67]. This would imply an even lesser dependency from traditional and polluting sources, and from the Combat Service Support, coupled with an optimized energetic consumption and increasing operational range and autonomy. The enabling and underpinning element is an energetic complex allowing the coexistence or the dynamic, immediate, and transparent switching of the three interoperable

[67] D. Panebianco, G. Rizzo, M. Ruggieri, E. Trenta and Gabinetto del Ministro della Difesa…, cit.

roles: Producer, Provider, and User[68]. The Producer has the capacity to generate energy by itself without resorting to external sources[69]. The Provider has the capacity to transfer the energy produced to the consumer, or User.

Assets and infrastructures energetically neutral will be much more efficient and effective in highly environmentally hostile Operational Theatres while maintaining full warfighting readiness. At the same time, they will grant operational advantage in operational scenarios of growing complexity from natural resources standpoint, like A2AD-ing energy resources, or natural disasters or catastrophe, or from the ever-increasing dependency of military technology from energetic sources. The broader strategic-operational implication is that energetically neutral Forces will be able to be seen as "part" of the environment instead of "operating in" the environment. Adversaries, opponents, and actors might find themselves mistaking a soldier for a bush, an aircraft for clouds, an aircraft carrier for waves of the ocean.

To reach this level of environmental integration and attunement, there are four technological pillars. The first two are Femtotechnology and Convergent Biology, as described before. The third is about energetic materials and multipurpose alloys: in the Fourth Offset, we will have energy storage, conversion, and production directly in the alloy. The effect might be like an armor plating with solar cells or batteries integrated, with the game-changing exception that there would be nothing else than raw "energetic steel".

The last is compact nuclear fusion: being able to equip our assets with a source of unlimited, clean, and high peak power source would provide an unlimited operational range, power, and even concealment when talking about submarines.

---

[68] Be they infrastructure, asset, or both. This concept is along the lines of the Smart Grid paradigm, that when extended to an Operational Theater becomes a Smart Battlefield Grid of Everything.

[69] E.g IoT devices or wireless sensor networks, that source energy by transforming light, heat, external movement in electricity.

Antifragility

Some things benefit from shocks; they thrive and grow when exposed to volatility, randomness, disorder, and stressors and love adventure, risk, and uncertainty. Nevertheless, despite the ubiquity of the phenomenon, there is no word for the exact opposite of fragile. Let us call it antifragile. Antifragility is beyond resilience or robustness. The resilient resists shocks and stays the same; the antifragile gets better. Antifragility is a concept explored by Nassim Taleb[70], describing a quality exhibited by complex systems. It is defined as "a convex response to a stressor or source of harm (for some range of variation), leading to a positive sensitivity to increase in volatility (or variability, stress, dispersion of outcomes, or uncertainty, what is grouped under the designation "disorder cluster"). Likewise fragility is defined as a concave sensitivity to stressors, leading to a negative sensitivity to increase in volatility. The relation between fragility, convexity, and sensitivity to disorder is mathematical, obtained by theorem, not derived from empirical data mining or some historical narrative. It is a priori"[71].

The classical example of antifragile system is muscles. Muscles grow as a result of repeated stress. With muscles, the potential downside due to stress and its retinue is lower than the potential upside of the increase in strength and stamina.

Antifragility is thus the embracing and weaponization of complexity.

If it is possible for systems to benefit from shocks, and becoming more robust as a result, the idea of injecting faults on purpose becomes a way to achieve the advantage. It is helpful to think of a vaccine or a flu shot where the body is injected with a small amount of a potentially harmful foreign body in order to prevent illness. And in fact, there is a discipline called Chaos Engineering centered around this idea. Chaos Engineering is

---

[70] N.N. Taleb, *Antifragile: Things That Gain from Disorder*, Random House, 2012.

[71] N.N. Taleb, "Philosophy: 'Antifragility' as a mathematical idea", *Nature*, vol. 494, no. 7438, 2013, February 2013, p. 430.

the discipline of experimenting on a distributed system in order to build confidence in the system's capability to withstand turbulent conditions in production[72]. It is used to build such immunity in technical systems by injecting harm (like latency, CPU failure, or network black holes) in order to find and mitigate potential weaknesses. These experiments have the added benefit of helping teams build a Pavlov reaction in resolving outages, much like a fire drill. By breaking things on purpose unknown issues surface that could impact our assets and Forces.

Chaos engineering is a technique to create antifragility. That is, if it is possible to evolve toward systems that survive that kind of chaos, then those systems will exhibit antifragility. However, one caveat: antifragility is not a universal or omni-dimensional characteristic[73]. Chaos engineering causes the system to evolve toward antifragility toward those kinds of stresses. Antifragile systems might benefit from variability, but not any variability. A system cannot be universally antifragile similar to how it cannot resist any failure.

The path towards evolving antifragility into a characteristic of socio-technical systems and assets for the future Forces is not all uphill. We already have a "Third Offset signpost": multi-purpose-by-design, namely assets capable of conducting many types of operations. They maximize utility and agility, with as few operational caveats as possible, without prejudice to full

[72] A. Basiri, "Chaos Engineering", *IEEE Software*, vol. 33, no. 3, May/June 2016, pp. 3541.

[73] For years, Netflix has been running an internal service called Chaos Monkey, which randomly selects virtual machine instances that host our production services and terminates them. Chaos Monkey's purpose was to encourage Netflix engineers to design software services that can withstand failures of individual instances. Chaos monkey kills AWS EC2 instances. The response is to build autoscaling, masterless clusters. That helps when machines are shut down, but not when whole regions do. Or when DNS fails., or when data gets corrupted, or when the marketplace changes. The potential downside of Chaos Engineering (occasional service interruptions) is smaller than the potential upside (better overall customer experience), up to a point (experiments causing severe damage that affect customers).

warfighting ability, effectively responding to dynamic and complex operational challenges as well as seizing opportunities with appropriate and timely actions.

Body-as-a-Node (ByN)

Through future Brain-Computer Interface (BCI) technology, we will have our body become a node of the network ("body-as-a-node")[74] and realize a full bio-cyber convergence. We will also be able to better communicate with people with severe disabilities, or critical illnesses, and even achieve basic dialogue with infants, pets, and wild animals. Taken one step further, a future version of the Internet may be formed through connecting minds instead of computers – the Braincloud. If the present trends are confirmed in the future, by the late 2040s we will all start plugging into wearable or implantable BCI technology. We will then need no smartphones at all – our minds will simply connect directly to the web to answer any databased question we come up with. At that point, intelligence will no longer be measured by the number of facts a user knows, but by the quality of questions a person can ask and the creativity with which they apply the knowledge accessible off the web, fully realizing the fundamental characteristic of the Imagination Age. Current trends confirmed, the Hybrid Generation – to be born between 2026-2045 – will grow up in a world with more than 200 billion devices connected and where neurotechnologies will enable users to interact with their environment and other people by thought alone. They will be learning how to sync their minds with the web, access information at will, control web-connected objects with their minds, and communicate brainto-brain with their peers, telepathically. Clarke's Third Law, "any sufficiently advanced technology is indistinguishable

[74] M. Ruggieri and G. Sannino, "Body as a Network Node: Key is the Oral Cavity", in S. Dixit and R. Prasad (eds.), *Human Bond Communication: The Holy Grail of Holistic Communication and Immersive Experience*, Wiley, 2017.

from magic"[75], fully applies here. At the same time, due to the massive exposition of physical and biological world in cyberspace, these systems will have to account for new means of protection of technology, data, and consciousness – like heartbeat, venous system, fMRI or "brainprints" as the top measures of security. The military use of this technology with undercover operatives or special forces will just be limited by the creativity in its employment. As a consequence, the entire capability spectrum in cyberspace will continue to be crucial for military and strategic advantage, and for the national resilience.

Algebraic Ethics

The ethical aspect of autonomous and intelligent systems is a critical concern today for the widespread acceptance of these kinds of systems throughout society and organizations. If, in the future, we will be able to reach a converged breakthrough in mathematics and philosophy giving us the ability to use formal language to encode ethics, this would solve the issue in its entirety. This goes along the lines of formal methods in computer science, i.e. mathematical approaches to solving software (and hardware) problems at the requirements, specification, and design levels. Being able to encode ethics in an explicit programming or formal semantics would bring mathematical soundness and provability to the complexity endowing this aspect.

Conclusion

What does all this mean, in practical terms? There are three main implications worth of notice.

First, technological change is as much substitution (Exponentiality) as it is about complementation (Convergence and Complexity). 80% of the assets and forces of tomorrow will

[75] A.C. Clarke, "Hazards of Prophecy: The Failure of Imagination", in A.C. Clarke, *Profiles of the Future: An Enquiry into the Limits of the Possible*, 1962.

be much like today, and just the 20% will be brand new. Of this 20%, the 80% (i.e. 16% overall) will be "innovatively" new and 20% (i.e. 4% overall) will be "disruptively and game-changing" new. Our responsibility is being able to illuminate as much as possible the possible futures to come so as to capture the right, albeit weak, signals from the future, and grant the technological surprise, superiority, and sustainability our future Forces will need to seize the initiative and consolidate strategic primacy.

Second, there is no rapid military advantage[76]: on the one hand, there is the constant struggle measurescountermeasures. The shaping force of convergence brings perpetually new and unexpected solutions to the problems our military advantages pose to our adversaries and opponents; we have to harness and shape it as well. On the other hand, systems evolve, significantly increasing their complexity, and thus requiring an exponentially larger effort to be realized, albeit bringing exponentially more powerful capabilities[77]. The complexity of new systems renders the advantage of backwardness is exponentially shallower than before, and the exponential compression of time induced by the shaping force of exponentiality is consumed in grappling with such complexity, which presents not just technological, but socio-technological, challenges. For instance, autonomous systems are definitively going to play an important role in the future of warfare. Some areas, given the widespread availability of data and the opportunities for constant updating such as ISR and logistics, are particularly suited for automation. However, integrating autonomous into existing force structures will be far from easy. This will represent a new challenge for future Forces. Future research will have to investigate more in-depth on those issues[78].

---

[76] A. Gilli and M. Gilli, "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage", *International Security*, vol. 43, no. 3, Winter 2018/19, pp. 141-189.

[77] G. Rizzo, *The Global Environment of 2060*, Air Force Space Command Space Futures Workshop, 2019.

[78] A. Gilli, *NATO-mation: Force Structure and the Atlantic Alliance in the Age of*

Third, it is of vital importance having a leadership highly evolved, aimed towards multi-dimensional, multi-disciplinary, integrated long-term thinking, leading a Military Instrument of Power able to anticipate and shape such trends, so that its resulting fragmented adaptation to the futures would instead become a transformation. Futures studies and foresight have to be in the new Leadership's toolbox, to position them in the best possible conditions to address in the most effective and efficient way the resources of the Military Instrument of Power, to ensure its credibility, networking, awareness, agility and resilience in the futures, so that soldiers, sailors, airmen or Marine, our men and women, will never face a fair fight.

Intelligence Machines, Research Paper, NATO Defense College, 2019.

3. Why 5G Requires New Approaches to Cybersecurity

Tom Wheeler, David Simpson

"The race to 5G is on and America must win", President Donald Trump said in April[1]. For political purposes, that "race" has been defined as which nation gets 5G built first. It is the wrong measurement.

The United States and Europe must "fire first effectively" in their deployment of 5G. Borrowing on a philosophy Admiral Arleigh Burke coined in World War II: Speed is important, but speed without a good targeting solution can be disastrous[2].

5G will be a physical overhaul of essential networks that will have decades-long impact. Because 5G is the conversion to a mostly all-software network, future upgrades will be software updates much like the current upgrades to smartphones. Because of the cyber vulnerabilities of software, the tougher part of the real 5G "race" is retooling how to secure the most important network of the XXI century and the ecosystem of devices and applications that sprout from that network.

---

* A first version of this chapter was published by the Brookings Institution on 3 September 2019 at https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

[1] R. Slayton, "Trump says 'America must win' the 5G race. Here's what you need to know", *The Washington Post*, 18 April 2019.

[2] Captain Wayne P. Hughes, Jr., USN (Ret.), *Fleet Tactics and Coastal Combat,* 2nd ed., U.S. Naval Institute Press, 2000, pp. 40-44.

Beyond the vulnerabilities of software, 5G networks have another vulnerability: a supply chain that circles the world. From hardware, software and firmware to the design of the apps and devices using the network, the 5G supply chain is composed of numerous participants. Each of these participants rely on the others, but none has cybersecurity as their core responsibility.

The new capabilities made possible by new applications riding 5G networks hold tremendous promise. As the United States and Europe pursue the connected future, however, they must place equivalent – if not greater – focus on the security of those connections, devices, and applications. To build 5G on top of a weak cybersecurity foundation is to build on sand. This is not just a matter of the safety of network users, it is a matter of national security – and a geopolitical imperative.

Hyperfocus on Huawei

Effective progress toward achieving minimally satisfactory 5G cyber risk outcomes is compromised by a hyperfocus on legitimate concerns regarding Huawei equipment in US and European networks. While the Trump administration has continued an Obama-era priority of keeping Huawei and ZTE out of domestic networks, for instance, it is only one of the many important 5G risk factors. The hyperbolic rhetoric surrounding the Chinese equipment issues is drowning out what should be a strong focus on the full breadth of cybersecurity risk factors facing 5G.

The purpose of this paper is to move beyond the Huawei infrastructure issue to review some of the issues that the furor over Huawei has masked. Policy leaders from Washington to Brussels should be conducting a more balanced risk assessment, with a broader focus on vulnerabilities, threat probabilities, and impact drivers of the cyber risk equation. This should be followed by an honest evaluation of the oversight necessary to assure that the promise of 5G is not overcome by cyber vulnerabilities, which result from hasty deployments that fail to sufficiently invest in cyber risk mitigation.

Such a review of 5G cyber threat mitigation should focus on the responsibilities of both 5G businesses and government. This should include a review of whether current market-based measures and motivations can address 5G cyber risk factors and where they fall short, the proper role of targeted government intervention in an era of rapid technological change. The time to address these issues is now, before the US and EU become dependent on insecure 5G services with no plan for how to sustain cyber readiness for the larger 5G ecosystem.

The after-the-fact cost of missing a proactive 5G cybersecurity opportunity will be much greater than the cost of cyber diligence up front. The NotPetya attack in 2017 caused $10 billion in corporate losses[3], with the combined losses at Merck, Maersk, and FedEx alone exceeding $1 billion. 5G networks did not exist at that time, of course, but the attack illustrates the high cost of such incursions, and it pales in comparison to an attack that would result in human injury or loss of life. Governments need to establish the conditions by which risk-informed cybersecurity investment up front is smart business for all 5G participants.

China is a threat even when there is not Huawei equipment in key telecommunications networks. From the successful exfiltration of highly sensitive security clearance data in the US Office of Personnel Management breach commonly attributed to China, to the ongoing China-linked threat actor campaign[4] in Europe and elsewhere, many of China's most successful attacks have taken advantage of vulnerabilities in non-Chinese applications and hardware and poor cyber hygiene. None of those threats disappear with a blanket ban on Huawei. The headline-grabbing focus on Chinese network equipment

[3] K.S. Nash, S. Castellanos, and A. Janofsky, "One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs", *The Wall Street Journal*, 27 June 2018.

[4] N. Drozdiak, N. Chrysoloras, and K. Donaldson, "EU Considers Response to China Hacking After U.K. Evidence, Sources Say", Bloomberg, 12 February 2019.

should not lull the West into a false sense of cybersecurity. In a world of interconnected networks, devices, and applications, every activity is a potential attack vector. This vulnerability is only heightened by the nature of 5G and its highly desirable attributes. The world's hackers (good and bad) are already turning to the 5G ecosystem, as DEFCON 2019 (the annual ethical "hacker Olympics") illustrated. The targets of this year's hacker villages included key parts of the 5G ecosystem such as: aviation, automobiles, infrastructure control systems, privacy, retail call centers and help desks, hardware in general, drones, IoT, and voting machines.

5G Expands Cyber Risks

There are five ways in which 5G networks are more vulnerable to cyberattacks than their predecessors:

- The network has moved away from centralized, hardware-based switching to distributed, software-defined digital routing. Previous networks were hub-and-spoke designs in which everything came to hardware choke points where cyber hygiene could be practiced. In the 5G software defined network, however, that activity is pushed outward to a web of digital routers throughout the network, thus denying the potential for chokepoint inspection and control.
- 5G further complicates its cyber vulnerability by virtualizing in software higher-level network functions formerly performed by physical appliances. These activities are based on the common language of Internet Protocol and well-known operating systems. Whether used by nation-states or criminal actors, these standardized building block protocols and systems have proven to be valuable tools for those seeking to do ill.
- Even if it were possible to lock down the software vulnerabilities within the network, the network is also being managed by software – often early generation

artificial intelligence – that itself can be vulnerable. An attacker that gains control of the software managing the networks can also control the network.

- The dramatic expansion of bandwidth that makes 5G possible creates additional avenues of attack. Physically, low-cost, short range, small-cell antennas deployed throughout urban areas become new hard targets. Functionally, these cell sites will use 5G's Dynamic Spectrum Sharing capability in which multiple streams of information share the bandwidth in so-called "slices" – each slice with its own varying degree of cyber risk. When software allows the functions of the network to shift dynamically, cyber protection must also be dynamic rather than relying on a uniform lowest common denominator solution.
- Finally, of course, is the vulnerability created by attaching tens of billions of hackable smart devices (actually, little computers) to the network colloquially referred to as IoT. Plans are underway for a diverse and seemingly inexhaustible list of IoT-enabled activities, ranging from public safety things, to battlefield things, to medical things, to transportation things – all of which are both wonderful and uniquely vulnerable. In July, for instance, Microsoft reported that Russian hackers had penetrated run-of-the-mill IoT devices[5] to gain access to networks. From there, hackers discovered further insecure IoT devices into which they could plant exploitation software.

Fifth-generation networks thus create a greatly expanded, multidimensional cyberattack vulnerability. It is this redefined nature of networks – a new network "ecosystem of ecosystems" – that requires a similarly redefined cyber strategy. The network,

[5] D. Goodin, "Microsoft catches Russian state hackers using IoT devices to breach networks", *Ars Technica*, 8 June 2019.

device, and applications companies are aware of the vulnerabilities and many are making, no doubt, what they feel are good faith efforts to resolve the issues. The purpose of this paper is to propose a basic set of steps toward cyber sufficiency. It is our assertion that "what got us here won't get us there".

Fifth-generation networks create a greatly expanded, multidimensional cyberattack vulnerability. Therefore, the redefined nature of these networks requires a similarly redefined cyber strategy.

5G service providers are the first ones to insist that 5G will underpin radical and beneficial transformation in modern life. At the same time, these companies have publicly worried about their ability to address the totality of the cyber threat and have described the future challenge in disturbingly blunt terms. For example, President Trump's National Security Telecommunications Advisory Committee (NSTAC) – composed of leaders in the telecommunications industry – told him in November, 2018[6], "The cybersecurity threat now poses an existential threat to the future of the [n]ation".

The nature of 5G networks exacerbates the cybersecurity threat. Across the US and Europe, consumers, companies, and cities seeking to use 5G are ill-equipped to assess, let alone address, its threats. Placing the security burden on the user is an unrealistic expectation, yet it is a major tenet of present cybersecurity activities. Looking to the cybersecurity roles of the multitude of companies in the 5G "ecosystem of ecosystems" reveals an undefined mush. Corporate efforts will not close the cyber gap as 5G greatly expands both the number of connected devices and the categories of activities relying on 5G. This general dissonance is further exacerbated by positioning Chinese technological infection of US and European critical infrastructure as the essential cyber challenge before us. The truth is that it's just one of many.

---

[6] The president's National Security Telecommunications Advisory Committee, *NSTAC Report to the President on a Cybersecurity Moonshot*, 14 November 2018.

What Have We Learned Thus Far?

5G has challenged traditional assumptions about network security and the security of the devices and applications that attach to that network. As officials of the US Federal Communications Commission (FCC), the authors struggled to deal with these challenges only to be confronted by:

- Industrial-era procedural laws that make rulemaking activity cumbersome and non-rulemaking activity less than optimal.
- The incentive of bad actors to overcome any solution that is typically greater than the incentive to maintain the protection.
- Industry stakeholder fear of exposing their internally identified risk factors at precisely the time when sharing information about attacks would be of greatest value for a collective defense.

At the same time, those who know the networks the best – the network operators – exist under business structures that are not optimal for effective risk reduction. As an FCC white paper concluded three years ago:

> As private actors, ISPs (internet service providers, such as 5G networks) operate in economic environments that pressure against investments that do not contribute to profit. Protective action taken by one ISP can be undermined by the failure of other ISPs to take similar actions. This weakens the incentive of all ISPs to invest in such protections. Cyber accountability therefore requires a combination of market-based incentives and appropriate regulatory oversight[7] where the market does not, or cannot, do the job efficiently.

[7] *FCC White Paper / Cybersecurity Risk Reduction*, Report, Federal Communications Commission, Public Safety & Homeland Security Bureau Federal Communications Commission, David Simpson, Rear Admiral (ret.) USN Bureau Chief, 18 January 2017.

Although the white paper was published by a US agency, its principle finding – that market forces alone would not address society's cyber risk interests – holds equally in the European Union as well. The fundamental issue is that in the larger digital ecosystem, the motivation to solve the problem generally gets worse when consumers do not link a purchasing decision with a cyber risk outcome. This is all too often the case in both the US and Europe, as service providers as well as device and application vendors do not make meaningful security differentiators public and don't compete on any verifiable security indicators.

In 2016, for instance, hackers shut down major portions of the internet by taking control of millions of low-cost chips in the motherboards of video security cameras and digital video recorders. That the internet could be attacked this way reflected the reality of digital supply chains: Because consumers didn't consider cybersecurity in their purchase decisions of low-cost connected devices (they were the means, not the target of the attack), retailers didn't prioritize security in their decisions of what to stock. As a result, manufacturers didn't emphasize cyber in the components they purchased and thus chip and motherboard manufacturers did not include cyber protections in their product. None of companies defined a role for themselves for sustaining post-purchase product cyber readiness and, by and large, that's still the case.

New industry verticals are bringing 5G-enabled capabilities to a market where good faith efforts are insufficient. There is no evidence that the business priorities of the suppliers of devices and applications are any different than those attributed to network operators in the FCC report. A 2018 report[8] by the Trump administration's Council of Economic Advisers, for instance, warned of, "underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment".

[8] White House, National Security and Defense, *CEA Report: The Cost of Malicious Cyber Activity to the U.S. Economy*, 16 February 2018.

None of this suggests that the march to the benefits of 5G should be suspended. It does, however, suggest that the *status quo* approach to 5G should be challenged. Continuation of corporate and governmental policies that are not keeping up with today's cyber risk do not bode well for a volumetric expansion of the attackable network and data surface of 5G networks. There is a crying need for coordinated efforts to achieve targeted expectations.

Two Keys to Winning the Real "5g Race"

The real "5G race" is whether the most important network of the 21stcentury will be sufficiently secure to realize its technological promises. Yes, speedy implementation is important, but security is paramount. To answer that overriding question requires new efforts by both business and government and a new relationship between the two.

The recommendations that follow are both important and not without cost. In normal times, such suggestions might be judged too much of a departure from traditional practices. These are not normal times, however. The outlook for a future that relies on 5G and other new digital pathways is cyber-defined. Both the United States and European Union have moved into a new era of non-kinetic warfare and criminal activity by nation-states and their surrogates. This new reality justifies the following corporate and governmental actions.

Key #1: Companies must recognize and be held responsible for a new cyber duty of care

The first of this two-part proposal is the establishment of a rewards-based (as opposed to penalty-driven) incentive for companies to adhere to a "cyber duty of care." Traditionally, common law established that those who provide products and services have a duty of care to identify and mitigate potential harms that could result. There needs to be a new corporate

culture in which cyber risk is treated as an essential corporate duty and rewarded with appropriate incentives, whether in monetary, regulatory, or other forms. Such incentives would require adherence to a standard of cyber hygiene which, if met, would entitle the company to be treated differently than other non-complying entities. Such a cyber duty of care includes the following:

- ✓ **Reversing chronic underinvestment in cyber risk reduction**. Proactive cyber investment today is the exception rather than the rule. For public companies, the Securities and Exchange Commission (SEC) and others are driving change from the corporate board-level on down through management. A favorite entrance point for cyberattacks, however, remains smaller companies, many of which are outside of the scope of these efforts. Unfortunately, the SEC's efforts impact only the less than 10% of American companies that are publicly owned[9]. At the very least, where companies have a role in critical infrastructure or provide a product or service that, if attacked, could imperil public safety, there must be the expectation that cybersecurity risks are being addressed proactively[10]. This should hold true as readily in Europe as the US.
- ✓ **Implementation of machine learning and artificial intelligence protection**. Cyberattacks on 5G will be software attacks; they must be countered with software protections. During a Brookings-convened discussion on 5G cybersecurity, one participant observed, "We're fighting a software fight with people" whereas the attackers are machines. Such an approach was like "looking through soda straws at separate, discrete portions of

[9] Intro to Private Companies, PrivCo,

[10] L.A. Gordon, M.P. Loeb, W. Lucyshyn, and L. Zhou, "Externalities and the Magnitude of Cyber Security Underinvestment by Private Sec tor Firms: A Modification of the Gordon-Loeb Model", *Journal of Information Security*, vol. 6, 2015, pp. 24-30.

the environment" at a time when a holistic approach and consistent visibility across the entire environment is needed. The speed and breadth of computer-driven cyberattacks requires the speed and breadth of computer-driven protections at all levels of the supply chain.

- ✓ **Shifting from lag indicators of cyber-preparedness (post-attack) to leading indicators**. A 2018 White House report[11] found a "pervasive" underreporting of cyber events that "hampers the ability of all actors to respond effectively and immediately". A recent EU report[12] has also expressed concerns about under-reporting. The 5G cyber realm needs to adopt leading indicator methodology to communicate cyber-preparedness between interdependent commercial companies and with government entities charged with oversight responsibilities. There are a number of good examples to pull from. Shared cyber risk assessments are increasingly a best practice for cyber-mature companies and their supply chain. Several accounting and insurance firms have developed lead metrics to inform cyber risk reduction investments and underwrite policies. The US Department of Homeland Security has resiliency self-assessment standards to motivate long-term community disaster preparedness improvement[13]. Such a model should be extended to the 5G cyber realm in order to shift oversight from lag indicators to lead indicators. A regular program of engagement with boards

[11] White House, Economy & Jobs, *Fighting Cybersecurity Threats to the Growing Economy*, 21 February 2018.

[12] European Court of Auditors, *Challenges to effective EU cybersecurity policy*, Briefing Paper, March 2019.

[13] While the authors do not want to understate the shortfalls associated with the NIMS self-assessment model and lack of federal engagement at the regional level to assess actual NIMS implementation, we do want to note that a decade in, NIMS has succeeded in establishing a common language and investment framework for long-term steady improvements to resiliency in over 10,000 jurisdictions across the country.

and regulators using cybersecurity lead indicators will build trust, accelerate closing the 5G readiness gap and lead towards more constructive outcomes when cyber attackers do succeed. Underreporting of lag indicators should be addressed, but with the primary purpose of closing the feedback loop, improving the quality of lead measures and the investment decision process they inform.

- ✓ **Cybersecurity starts with the 5G networks themselves**. While many of the large network providers building 5G are committing meaningful resources to cyber, small- and medium-sized wireless ISPs have been hard pressed to rationalize a robust cybersecurity program. In the US this manifestation occurred, not in major networks, but in small rural providers, some of which have fewer than 10 employees and can't afford a dedicated cyber security officer or a 24/7 cyber security operations center. 5G cybersecurity is not, however, a matter of size. Even the smallest providers will be offering 5G services and interconnecting with 5G networks. Unfortunately, in the US about one-third of these small companies have ignored government warnings about the use of Huawei equipment and are now petitioning Congress to pay for their poor decisions and pay to replace the non-Chinese equipment. Any replacement must include the expectation that the companies will establish sufficient cybersecurity processes that sustain protections. All the networks that deliver 5G 0 whether big brand names, small local companies, wireless ISPs, or municipal broadband providers 0 must have proactive cyber protection programs.
- ✓ **Insert security into the development and operations cycle**. For many application developers, a core agile development tenet has been sprinting to deploy a minimum viable product, accepting risk, and committing to later providing consumer-feedback-driven upgrades

once the product gains a following. Software companies and those providing innovative, software-based products and services are beginning to insert cybersecurity in the process as a design, deployment, and sustainment consideration for every new project. Such security by design should be a minimum duty of care across the commercial space for innovations in the emerging 5G environment.

- ✓ **Best practices**. In the US the National Institute for Standards and Technology (NIST) Cybersecurity Framework[14] has established five areas for best practice cybersecurity management that could become the basis of industry best practices: Identify, protect, detect, respond, and recover. For instance, NIST's "identify" initiative focuses on determination of a company's cyber universe, threats, and vulnerabilities in order to identify cyber risk reduction investments. Regardless of whether they adopt the NIST framework specifically, both the United States and European Union should establish cybersecurity standards of expected performance and accompanying incentives for their adoption by companies. While industry-developed best practices are a step in the right direction, they are only as strong as the weakest link in the industry and continue to place the burden on poorly informed consumers to know whether the best practices are being fulfilled.

Unfortunately, publication of optional cybersecurity best practices without full industry buy-in may be an attempt at responsible behavior and good public relations, but often do little to change the cyber risk landscape. The 5G commercial sector needs to acknowledge the limits of consumer-based actions, own the residual risk, and work together with government oversight to assign cross-sector mitigation responsibilities.

[14] https://www.nist.gov/cyberframework

Key #2: Government must establish a new cyber regulatory paradigm to reflect the new realities

Current procedural rules for both US and European agencies were developed in an industrial environment in which innovation and change – let alone security threats – developed more slowly. The fast pace of digital innovation and threats requires a new approach to the business-government relationship.

- ✓ **More effective regulatory cyber relationships with those regulated**. Cybersecurity is hard, and we should not pretend otherwise. As presently structured, government is not in a good position to get ahead of the threat and determine detailed standards or compliance measures where the technology and adversary's activities change so rapidly. A new cybersecurity regulatory paradigm should be developed that seeks to de-escalate the adversarial relationship that can develop between regulators and the companies they oversee. This would replace detailed compliance instructions left over from the industrial era with regular and fulsome cybersecurity engagements between the regulators and the providers at greatest risk as determined by criticality, scale (impact), or demonstrated problems (vulnerabilities) built around the cyber duty of care. It would be designed to reward sectors where participants have organized and are clearly investing ahead of failure to address risk factors. Conversely, where sectors are ignoring cyber risk factors, graduated regulatory incentives can change corporate risk calculus to address consumer and community concerns. These activities would be afforded confidentiality and not be used by themselves to discover enforcement violations, but instead to help both regulators and the regulated better spot trends, best practices, and collectively and systematically improve their sector's approach to cyber risk. NATO and national security agencies can have a role in this, but at the end of the day, the balance between security, innovation, corporate means, and market factors is inherently regulatory.

- ✓ **Recognition of marketplace shortcomings**. Economic forces drive corporate behavior. Of course, there are bottom-line-affecting costs associated with cybersecurity. Even when such costs are voluntarily incurred, however, their benefits can be undone by another company that doesn't make the effort. The first of this paper's two recommendations suggests what companies can do to exercise their cyber duty of care. History has shown, however, that the carrot accompanying such efforts often needs the persuasion of a standby stick. This is only fair to those companies that step up to their responsibility and should not be penalized in the marketplace by those that do not step up. A rewards-based policy would amplify the value of cyber duty of care participation, especially when others fall short. It would also provide forward-looking incentive for risk reduction and a more useful feedback loop when breaches invariably occur.
- ✓ **Consumer transparency**. Consumers have little awareness and no insight with which to make an informed market decision. The situation is analogous to the forces that resulted in the establishment of nutritional labeling for foods. Consumers should be given the tools with which to make informed decisions. "Nutritional labeling" about cyber risks or a cyber version of Underwriters Laboratories' self-certification will help focus the attention of all parties on its importance.
- ✓ **Inspection and certification of connected devices**. For years, the FCC has overseen a program to certify that radio-signal-emitting devices do not interfere with authorized use of the nation's airwaves. Whether cellphones, baby monitors, electronic power supplies, or Tickle Me Elmo, the FCC assures the design and assembly of transmitting devices are within standards. Similar agencies have done the same in Europe. Industry then organizes underneath that construct to

self-certify devices in a cost-effective means baked into their production and distribution processes. At the time of the 2016 DYN attack that took control of millions of video cameras, the authors proposed a similar regimen to review the cybersecurity of connected devices. Why should radio networks be protected from harmful equipment, but not 5G networks[15] from cyber-vulnerable equipment?

- ✓ **Contracts aren't enough**. Governments often seek to use their purchasing power to impose cybersecurity requirements. This is an important, proven practice, but it can only go so far. Such acquisition policies, for instance, do not reach non-government suppliers that in an interconnected network can wreak havoc by simply connecting to the network. Typically, small and medium 5G network providers are not bound by any of these government contracts.
- ✓ **Stimulate closure of 5G supply chain gaps**. In both the US and Europe, review of mergers and acquisitions has typically failed to appreciate the potential negative impact on critical supply chains. Moving companies and processes offshore or to joint ventures with non-democratic foreign ownership/control has created wholesale gaps in the supply of crucial 5G components and the absence of procurement options with the domestic US and Europe. Country of origin/ownership concerns must become relevant to both the corporate calculus that led to offshoring purchase decisions as well as to the market conditions that led to the destruction of a national capability in the first place. 5G supply chain market analysis must be continuous with regular engagement between regulators, industry, and the executive and legislative branches to properly incentivize globally competitive domestic sourcing alternatives.

[15] Federal Communications Commission (FCC), FCC Response 12-05-2016.

- ✓ **Re-engage with international bodies**. At present, the standards setting process for 5G is governed by the 3rd Generation Partnership Project (3GPP), an industry group that makes decisions by consensus based on input from its members, including Chinese 5G equipment companies. (Huawei reportedly made the most contributions to the 5G standard)[16]. The Obama FCC engaged directly with 3GPP to identify public safety and cybersecurity risk considerations applicable to the US market. It additionally opened a notice of inquiry to ask the nation's best technology brains how to implement cybersecurity risk reduction as part of the development and deployment cycle. The move was opposed by some industry associations and the Republican commissioners. Shortly after the beginning of the Trump administration, the new FCC cancelled the Obama FCC's cyber initiatives. Both the US and EU should have policy-maker engagement with 3GPP. There needs to be informed third-party oversight early in the 5G industry's design and deployment cycle in order to prioritize cyber security. Governments should have some degree of agency in the process. This will allow for earlier issue identification and the opportunity to submit concerns, without changing the basic governance of standards setting. The representatives of the citizens of the US and EU should have the option to escalate engagement on matters of national security and public safety concern.

[16] T. Pohlmann, "Who is leading the 5G patent race?", *IAM*, 12 December 2018.

Conclusion

In March, the European Commission released a recommendation[17] on the cybersecurity of 5G networks, culminating in a major new report[18] on 5G and cybersecurity this October. In July, the US Senate, led by Republicans, introduced legislation[19] instructing the Trump administration "to develop a strategy to ensure the security of next generation mobile telecommunications systems and infrastructure". Key leadership in both the EU and US recognize the full peril that 5G introduces, and the need for whole-of-government responses.

Early generation cyberattacks targeted intellectual property, extortion, and hacked databases. Today, the stakes are even higher as nation-state actors and their proxies gain footholds in critical infrastructure to create attack platforms lying in wait. Companies that provide critical network infrastructure or provide products or services connected to it represent the likely and potentially most dangerous enemy course of action in the ongoing cyber cold war.

"If you're asking me if I think we're at war, I think I'd say yes", the former commandant of the Marine Corps, Gen. Robert Neller, told an audience in February[20]. "We're at war right now in cyberspace. […] They're pouring over the castle walls every day". While the adversaries of the US and Europe see positive outcomes for high-profile direct attacks, they also are perfecting less-risky positive outcomes in a steady pace of low-level attacks intended to erode public confidence in cyber critical infrastructure and the digital economy it underpins. The low-intensity cyber war is already ongoing as non-democratic regimes in Moscow and Beijing risk very little in these attacks but stand to gain much.

---

[17] European Commission, *Cybersecurity of 5G networks*, 26 March 2019.

[18] European Commission, *Member States publish a report on EU coordinated risk assessment of 5G networks security*, 9 October 2019.

[19] S.893 - Secure 5G and Beyond Act of 2019, Congress.gov.

[20] G.I. Seffers, "Kinetic Weapons Remain a Priority as Cyber War Rages", *Signal*, 15 February 2019.

Into this attack environment has come a software-based network built on a distributed architecture. With its software operations per se vulnerable, and a distributed topology that precludes the kind of centralized chokepoint afforded by earlier networks, 5G networks will be an invitation to attacks. Given that the cyber threat comes through commercial networks, devices, and applications, the 5G cybersecurity focus must begin with the responsibilities of those companies involved in the new network, its devices, and applications. The cyber duty of care for those involved in 5G services is the beginning of such proactive responsibility.

At the same time, both the European Union and the United States have their own responsibility to create incentives for 5G companies to focus on the cyber vulnerabilities they create. This is especially the case when there may be a corporate or marketplace lack of motivation to prioritize a maximum cyber effort. As outlined in this paper, this will necessitate replacing the rigid industrial-era relationship between government and business with more innovative and agile means of dealing with the shared problem.

Yes, the "race" to 5G is on – but it is a race to secure the shared future of the United States and Europe.

4. AI in the Aether: Military Information Conflict

Tom Stefanick

Since the advent of modern deep learning earlier this decade, there has been significant discussion of artificial intelligence and information warfare. In his paper, titled *"Mind Hacking": Information Warfare in the Cyber Age*, Fabio Rugge[1] discusses the growing strategic importance of the "information space" as a regime of conflict in military operations. "Operations in this domain are central to Russia's security strategic thinking, featuring prominently in its 'New Generation War' military doctrine"[2]. In early 2019, ISPI highlighted a different element of warfare with the publication of "Artificial Intelligence: A New Era of Warfare" by John R. Allen, President of the Brookings Institution. In his piece, Allen warns that the synergy of artificial intelligence (AI), analytic methods applied to huge data sets, and super-computing "represents the core ability to remain competitive in an era of great power conflict"[3]. I will extend those discussions to electronic warfare and it's central role in NATO's ability to deter Russian intimidation and aggression.

---

* This chapter is part of a forthcoming book on artificial intelligence and how it may impact military capabilities. The book will be published by Brookings Press in late 2020.

[1] F. Rugge, *"Mind Hacking": Information Warfare in the Cyber Age*, ISPI Analysis no. 319, ISPI, January 2018.

[2] Ibid., p. 1.

[3] J.R. Allen, "Artificial Intelligence: A New Era of Warfare," *The World in 2019*, ISPI Dossier, January 2018.

Electronic warfare (EW) systems directly impact the information space of military conflict. With the increasing automation of EW systems, modern AI algorithms are being investigated to determine their value as a component of new EW systems. I discuss the ways in which modern AI algorithms may or may not be incorporated into EW systems, and prospects for the sudden emergence of a Russian AI-driven EW capability. I will also highlight the serious dilemma created by effective EW, as it can inhibit human control over unmanned weapons, while at the same time bolstering NATO's deterrence of Russia. To begin this analysis, I walk through some explanations of AI and EW before returning to their importance for NATO.

What is Artificial Intelligence?

The term "artificial intelligence" has had no fixed meaning since it first entered the computer science lexicon in the late 1950s. The definition used here is narrower than that typically used in the current policy and futurist literature, and is proposed as a baseline to focus discussion. However, the definition is sufficiently broad to encompass current research and implementations that are likely to have practical national security implications within the next 20 years. "Machine learning" is a term that encompasses a very wide set of algorithms – including modern AI algorithms – which perform a range of tasks as described below. Machine learning, as the much broader concept, includes algorithm designs based on a much wider range of mathematical principles than the principles underlying modern AI algorithms.

The surge of excitement, apprehension, and imaginative speculation about the impacts of artificial intelligence (AI) since around 2014 appears to follow upon a rapid sequence of newsworthy technical accomplishments. These accomplishments include highly accurate image, video, and face recognition; improved prediction of machinery degradation; language translation and sentiment/topic detection in text; recommendations

for the next video to watch; reliable voice recognition and automatic dialog generation; synthetic image, video and voice generation of individuals ("deep fakes"); control of complex physical systems; and high-level game play against opponents in board games and computerized warfare games. Many of these algorithms are widely available as open-source software.

Recent AI algorithm advances are the product of a convergence of three elements that have been a long time in development: advances in algorithms based on extremely large neural networks with millions of adjustable parameters, adaptation of inexpensive parallel-processing computer chips including graphical processing units (GPUs) and other designs, and the ever-expanding availability of online data generated by humans and sensing devices through all forms of social media and other online services.

Modern AI as defined here comprises two main classes of algorithms: deep neural networks and deep reinforcement learning algorithms. The foundational modern AI algorithm is the deep neural network (DNN), which may be configured in a large number of ways depending on its function and the data it is using. Deep neural networks are built up from a very large number of simple computational sub-functions, which in the aggregate have millions to hundreds of millions or more adjustable parameters. These DNNs can approximate virtually any complex relationship between inputs and outputs by using large data samples to adjust these parameters depending on the intended use. New DNN architectures and approximation methods are invented regularly, and no attempt is made to reference them all explicitly.

The second group of algorithms driving modern AI – deep reinforcement learning (deep RL) – is designed to interact with complex environments such as game systems or control variables for physical systems. As the name suggests, deep RL algorithms incorporate deep neural networks to store the information they extract from their environments. As deep RL algorithms explore these environments by moving through possible

system states, they receive data on how actions result in changes to the environment, and they also reap a reward signal that guides their behavior. Over many – often millions – of interactions with the same environment and reward rules, these deep RL algorithms compute approximate solutions for operating in that environment and store these solutions in the embedded DNNs.

As a final note regarding definitions, it is recommended that discussion of autonomous systems – physical or computational – be clearly distinguished from AI as defined above. Any number of algorithms, including but not exclusively AI algorithms may enable highly effective autonomous systems. Moreover, physical autonomous systems are constrained by physical limitations (e.g. energy) that must be considered when assessing their capabilities. The electronic warfare systems of all modern militaries are heavily reliant on autonomous algorithms which have been refined over decades.

It is noteworthy that to the extent that EW systems are capable of disrupting communications systems of the adversary's remotely piloted vehicles – the very communications that allow human control over the weapons on those unmanned vehicles – that the assurance of human control over those weapons diminishes. DARPA's Collaborative Operations in Denied Environment (CODE) is an example of a technological response to the challenges of modern EW[4]. As unmanned vehicles continue to enter the arsenals of modern states in parallel with effective EW systems, military planners will face a choice: allow fleets of remotely-piloted unmanned vehicles to become ineffective, or push some of the decision-making processes into the unmanned vehicles themselves, moving them toward lethal autonomous weapon systems[5]. Electronic warfare R&D may

[4] S. Wierzbanowski, "Collaborative Operations in Denied Environment (CODE)", DARPA.

[5] This point of view is also articulated by K.D. Atherton: "To understand autonomous weapons, think about electronic warfare", C4ISR NET, 15 November 2018.

point to a way out of this dilemma, through the development of jam-proof communications and navigation algorithms for unmanned vehicles. However, this sets up a spiral of technological racing in the EW domain that will take on increasing importance.

What is Electronic Warfare?

Military operations are enabled by data transmitted through several media, but none of these media are more important than the electromagnetic (EM) spectrum. In particular, EW refers to data propagating through the atmosphere and space between transmitting and receiving antennae and electronics. The EM spectrum includes gamma and X-rays, to visible light, and on to infrared and radio waves used for communications and radar. Most military communications systems rely on EM transmissions and most sensors that are used to detect and track targets use EM signals – the undersea environment being a major exception[6]. Remote sensors that detect objects at a distance using EM signals are central to modern military and intelligence capabilities. These may be autonomous sensors, such as space-based sensors on satellites, sensors on aircraft (manned or unmanned), sensors on ships, submarines, or ground sensors.

Military means for manipulating or using the EM signals of an adversary – electronic warfare – have developed in tandem with detection and communication measures, giving rise to technological struggle between opponents within the electromagnetic spectrum. For the US military, the definitive explanation of EW is found within the Joint Chiefs of Staff (JCS) Joint Publication 3-13 series on Information Operations[7] – of which

[6] Most practical EM waves do not propagate in the ocean, so acoustic sensors and communications are used in that environment.

[7] Joint Publication 3-13 Information Operations, 27 November 2012, Incorporating Change 1, 20 November 2014. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

EW (Joint Publication 3-13.1) is a part[8]. The various functions of EW are placed in three categories: electronic attack, electronic protection, and electronic warfare support. Examples of EW functions include: directed energy to attack and disable personnel, facilities or equipment; actions taken to protect one's own forces from directed energy; jamming radar and communications; injecting deceptive data into radars and communications; and finding the location of and adversary's communication and radar emitters. Thus, the term "electronic warfare" encompasses powerful offensive weapons for destroying electronics and jamming GPS signals that every person relies on for safety, as well as defensive systems to protect one's own communications. Data links exist between almost any combination of dismounted soldiers, ground vehicles, satellite, aircraft, ships, land sites, submarines with near-surface antenna, etc. These links enable coordination and command and control of forces across echelons and across geographic regions.

There is concern within NATO leadership that electronic warfare capabilities have not received the attention that they need to, largely due to the fact that recent conflicts have not included EW threats. The primary use of EW in Iraq and Afghanistan was to jam the remote detonators for improvised explosive devices, and NATO's adversaries in those conflicts had little EW attack capability. An excellent summary of the NATO EW situation was recently provided by Commander Malte von Spreckelsen, Chief Policy Section, NATO Joint Electronic Warfare Core Staff:

> In the face of such limited opposition, coalition and Alliance forces could use the electromagnetic spectrum with few limitations. This enabled the uninterrupted use of the Global Positioning System (GPS) for navigation and heavy reliance on systems like the Blue Force Tracker. Friendly forces enjoyed virtually unhindered communications means for command and

[8] Joint Publication 3-13.1 Electronic Warfare, 8 February 2012, https://fas.org/irp/doddir/dod/jp3-13-1.pdf

> control. Old, valuable concepts such as radio discipline, electromagnetic signature control, and frequency hopping were less important in these environments. Therefore, over the years, the focus and devotion towards EW faded within NATO. Policies, plans, and doctrine slowly, but steadily, became outdated. EW training in forces throughout NATO lost focus and EW skills atrophied. Additionally, new, more publicly accessible capabilities like "Cyberwarfare" emerged and dragged a lot of effort, resources, and attention away from traditional EW, which was to some degree viewed as the purview of high-end militaries and a threat that had faded with the demise of the Soviet Union[9].

Indeed, cyberwarfare has become a critical element of military communications, and has the additional characteristic that every individual in modern societies are connected to the internet and is influenced by the cognitive impact of social media interfaces. However, military EW and EW countermeasures are an essential component in the management of conflict, as the data the flows on networks directly impact understanding of the moment-by-moment military picture.

The importance of EW has steadily grown as modern military command and control has emphasized connectivity through all echelons. The United States led the way in emphasizing Network-Centric Warfare since the 1990s[10]. After the end of the Cold War, and through the period of relative US dominance in controlling worldwide communications in air, space, and then the Internet, it was natural for future-looking US military technologists to envision a world in which all levels of military operations had full access to all data all the time. However, as the vulnerabilities of the Internet-linked data flows became more apparent, the risks of corrupted data, deceptive data, or not data at all became clear.

---

[9] Commander M. von Spreckelsen, NATO Joint Electronic Warfare Core Staff, "Electronic Warfare – The Forgotten Discipline", Joint Air Power Competence Center.

[10] A.K. Cebrowski and J.J. Garstka, "Network Centric Warfare: Its Origin and Future", Proceedings of the Naval Institute, vol. 124, no. 1, January, 1998, pp. 28-35.

How Does Electronic Warfare Relat to Information Warfare?

To discuss information warfare, it is helpful to distinguish the information environment in military operations from the physical. The physical domains of warfare are ground, maritime, air, and space. Platforms (tanks, ships, aircraft, satellites) as well as the warriors, sensors, and weapons they carry operate within this physical environment, and are necessarily constrained by laws of physics. The bridge between the physical domains and the information domain is data. Data is generated by sensors, people, and computer hardware. For the purposes of this analysis, the physical elements of data flow are computing systems, cables, transmitters, receivers, and other objects that enable the flow of data[11]. Data is stored on physical devices and transmitted through the physical world: as electrical signals, light signals in fiber optic cables, and electromagnetic waves through air and space. Data transmission and reception are themselves constrained by physics.

Information, on the other hand, is related to cognitive processes such as inference and decision-making. Information is carried by data, but is not data itself: information has to be extracted from data, interpreted, and used in the context of making an inference about the state of the world, and making a decision based on inference[12]. The US Joint Chiefs of Staff have

[11] From JP 3-13, the description is "The physical dimension is composed of command and control (C2) systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. It is the dimension where physical platforms and the communications networks that connect them reside. The physical dimension includes, but is not limited to, human beings, C2 facilities, newspapers, books, microwave towers, computer processing units, laptops, smart phones, tablet computers, or any other objects that are subject to empirical measurement. The physical dimension is not confined solely to military or even nation-based systems and processes; it is a defused network connected across national, economic, and geographical boundaries".

[12] Quoting from a standard graduate textbook on information theory, "The concept of information is too broad to be captured by a single definition". T. Cover

established some useful definitions and conceptual distinctions in Joint Publication 3-13 Information Operations:

> The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions which continuously interact with individuals, organizations, and systems. These dimensions are the physical, informational, and cognitive[13].

The cognitive dimension is clearly called out by JCS Doctrine as the most important of the three dimensions.

> The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information. It refers to individuals' or groups' information processing, perception, judgment, and decision making. These elements are influenced by many factors, to include individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies. Defining these influencing factors in a given environment is critical for understanding how to best influence the mind of the decision maker and create the desired effects. As such, this dimension constitutes the most important component of the information environment[14].

EW seeks to disrupt the physical means of data flow in order to impact the cognitive abilities of the adversary[15]. Electronic warfare is the physical part of a battle to degrade the adversary's command and control of their forces by disrupting data.

---

and J. Thomas, *Elements of Information Theory*, p. 13.

[13] Joint Publication 3-13, p. I-1…, cit.

[14] Ibid., p. I-3.

[15] The JP 3-13 also defines an "information dimension" of the "information environment", but that distinction will not be used here. It is described as follows: "The informational dimension encompasses where and how information is collected, processed, stored, disseminated, and protected. It is the dimension where the C2 of military forces is exercised and where the commander's intent is conveyed. Actions in this dimension affect the content and flow of information".

Algorithms are, by definition, automated means of manipulating data, and sophisticated signal processing algorithms are already at the heart of EW systems. Is there something special about the new modern AI algorithms that might significantly change this military function?

How Might Modern AI Algorithms Be Applied to EW?

Radars, navigation systems, and radio communications systems have been carefully designed over the decades to provide the maximum information and range. Even in the absence of EW, electromagnetic waves propagating through the atmosphere and space are disturbed by many effects. This has led designers to craft specialized signal patterns for communications, navigation, and radar signals that are well known, and tend to preserve the information content of the signal. Experts in signal processing can therefore develop highly effective algorithms using expert knowledge of how electronic communications systems are designed. In attempting to apply modern AI algorithms to the field of signal processing, the deep neural network learning-based algorithms must therefore compete against a mature field. An expert in the fields of signal processing as well as deep learning methods put it this way:

> Communications is a field of rich expert knowledge about how to model channels of different types, compensate for various hardware imperfections, and design optimal signaling and detection schemes that ensure a reliable transfer of data. As such, it is a complex and mature engineering field with many distinct areas of investigation which have all seen diminishing returns with regards to performance improvements, in particular on the physical layer. Because of this, there is a high bar of performance over which any machine learning (ML) or deep learning (DL) based approach must pass in order to provide tangible new benefits. In domains such as computer vision and natural language processing, DL shines because it is difficult to characterize real

> world images or language with rigid mathematical models. For example, while it is an almost impossible task to write a robust algorithm for detection of handwritten digits or objects in images, it is almost trivial today to implement DL algorithms that learn to accomplish this task beyond human levels of accuracy. In communications, on the other hand, we can design transmit signals that enable straightforward algorithms for symbol detection for a variety of channel and system models (e.g., detection of a constellation symbol in additive white Gaussian noise (AWGN)). Thus, as long as such models sufficiently capture real effects, we do not expect DL to yield significant improvements on the physical layer[16].

The above quote captures a very important idea in assessing how modern AI algorithms might affect military and intelligence systems in general. Current algorithms at the core of most modern military systems usually derive from well-founded theory based in mathematics and its sub-fields of probability, statistics, optimization, as well as decades of work in computer science. There is an enormous literature and experience base of applications of this theory – combined with clever heuristic thinking – that current military systems are based on. In each particular application where we think about the impact of modern AI algorithms, there will almost always be a range of alternative algorithms that have been crafted for the particular problem, integrated within tightly-designed systems, and operated successfully.

In order to forecast the extent to which modern AI algorithms might be incorporated into intelligence or military systems, including EW, it is critical to assess the data associated with these systems when they are in use. Modern AI algorithms used for classification of signals, such as deep neural networks, would require very large amounts of well-labeled signal data for parameter optimization prior to implementation. While this is

[16] T. O'Shea, *An Introduction to Deep Learning for the Physical Layer*, arXiv:1702.00832v2 [cs.IT], 11 Jul 2017. The author goes on to describe how applying modern AI algorithms to signal data can provide useful insights.

certainly possible, the modern EW environment is characterized by very agile systems, that can adapt and change. To the extent that a deep neural network is trained on less than the full range of possible data it might encounter, its performance will be uncertain.

Deep reinforcement learning (deep RL) algorithms might appear to be more readily adaptable to the EW problem, but in this case, the parameter optimization data is built up over very large numbers of interactions with the "adversary" system, with the introduction of appropriate reward signals. Unlike training a deep RL algorithm to play the game Go, or StarCraft II, in which the adversary plays by consistent rules millions of time, military EW does not allow for long, repeated engagements with fixed rules. There are cases of adversaries adapting rapidly to sophisticated EW by shifting tactics to different parts of the EM spectrum[17].

Nonetheless, it is very possible that there will be particular applications for military systems in which the attributes of modern AI algorithms will demonstrate improvements in the future. It is worthwhile, then to survey some of the recent international technical journals to assess some research directions pertinent to AI and EW.

Modern radar, communications, and EW signal processing developments have developed a common theme based on the concept of adaptation of the system to information gained from the environment. One of the prominent themes in this feedback-based view is espoused by Simon Haykin[18]. This research

---

[17] "As one example to illustrate the conundrum faced by the U.S., [the Joint-Improvised Threat Defeat Organization] spent $2.3 billion to develop an electronic signal jamming device to stop IED triggers that use two-way radios or garage door openers. In response, the insurgents switched to laser trigger devices, thereby negating the investment", R. Mordfin, *Insurgents are Learning to be More Effective on the Battlefield*, The University of Chicago, Harris Public Policy, 7 February 2018.

[18] S. Haykin, "Cognitive Radar: A Way of the Future", *IEEE Signal Processing Magazine*, January 2006, pp. 30-40. S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications", *IEEE Journal on Selected Areas in Communications*, vol.

represents only one of many active themes in modern research that is not related to deep neural network-based algorithms[19]. However, researchers have recently been applying deep neural networks to selected sub-problems within these EW domains. Some examples include: application of convolutional neural networks for improving direction-of-arrival estimates for EW systems[20], using deep neural networks to classify radar pulses based on images created by time-frequency images of the radar signals[21], competitive deep reinforcement learning-based methods for adapting ones' own communications to an EW environment where the opponent is using adaptive jamming[22], and other approaches based on applications of a wide array of algorithms to the automated confrontation between electronic systems.

A review of the technical literature from the US and China indicate that researchers are experimenting with application of modern AI algorithms to particular functions within the overall EW signal processing chain. There is a growing body of technical literature that is showing incremental improvements in the overall capabilities of EW processing chains. This is of course exactly what we would expect from any new technology as it is applied within complex systems with many stages and components. To date, however, there is no evidence of a major improvement in EW system capability driven by the introduction of deep neural networks or deep reinforcement learning. The

---

23, no. 2, February 2005, pp. 201-220.

[19] K. Bell, et. al. "Cognitive Radar Framework for Target Detection and Tracking", *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 8, December 2015.

[20] A. Elbir et al., "Cognitive Radar Antenna Selection via Deep Learning", *IET Research Journals*, pp. 1-10. Accessed via arXiv:1802.09736v3 [eess.SP], 4 February 2019.

[21] QU Zhiyu et. al., "Radar Signal Intra-pulse Modulation Recognition Based on Convolutional Denoising Autoencoder and Deep Convolutional Neural Network", *IEEE Access*, vol. 7, 2019, pp. 112339-112347.

[22] LI Yangyang et. al., "On the Performance of Deep Reinforcement Learning-Based Anti-jamming Method Confronting Intelligent Jammer", *MDPI Applied Sciences* (China), 2019, vol. 9, p. 1361.

fact that research in China is now applying modern AI algorithms to EW may be driven in part the incentives and funding available associated with the Chinese government's artificial intelligence goals[23].

Russia's Focus on Electronic Warfare

Russian military thinkers have long understood and theorized about the importance of information in all aspects of military decisions and operations[24]. Domains of military competition that have in the past been considered separately, such as space, electronic warfare, networked operations, and cyber operations are increasingly viewed as a seamless operational domain. The term "hybrid warfare – the use of proxies, disinformation, and other measures short of war"[25] has been associated with articles and speeches of General Valery Gerasimov, and termed the "Gerasimov Doctrine". Eugene Rumer of the Carnegie Institution places Gerasimov's statements into a longer historical context, articulated first by former foreign and prime ministry Yevgeny Primakov[26].

> Russia's military posture vis-à-vis NATO appears to be a calculated mix of hard power and hybrid warfare designed to deny NATO its advantages – the numerical superiority of allied militaries, technological superiority, an edge in air power, economic potential, and a long record of political cohesion and commitment to shared principles. Russia's posture suggests a country

[23] For a coherent explanation of how these incentives to work on AI-related matters operate within China, see M. Sheehan, "How China's Massive AI Plan Actually Works", Macro Polo, Chicago, IL, Paulsen Institute, 12 February 2018.

[24] V.V. Druzhinin and D.S. Kontorov, *Concept, Algorithm, Decision (A Soviet View)*, Chapter 3, Moscow, US Air Force, 1972.

[25] N. Ng and E. Rumer, *The West Fears Russia's Hybrid Warfare. They're missing the Bigger Picture*, Commentary, Washington DC, Carnegie Endowment for International Peace, 3 July 2019.

[26] E. Rumer, *The Primakov (Not Gerasimov) Doctrine in Action*, Washington DC, Carnegie Endowment for International Peace, 5 June 2019.

> that is realistic about its limited prospects to achieving superiority and is instead focused on denying its opponent's advantages – consistent with Primakov's vision[27].

For Russia, EW is a low-cost, low-risk means to inject uncertainty into NATO, as well as a means of assuring its own command and control in the face of NATO's technical superiority. Russia has been updating their EW systems, and has a recent history of using them in eastern Ukraine and Syria. Indeed, these uses of EW have provided NATO with insights on Russian tactics and capabilities[28]. Russia's response to superior NATO capabilities[29] has been significant, but the offensive capabilities of Russian EW have also been exaggerated. A great deal of Russia's investment and deployment of EW capabilities has been to defend and protect their own communications links. The most recent Russian uses in Syria were most likely focused on force and base protection[30]. On the offensive side, EW remains a very cost-effective counter to NATO capabilities that rely on communications, sensor networks, and targeting data connected from sensors to weapon systems[31].

How does the steady buildup of EW capabilities by Russia impact on NATO's ability to deter adventurism on a small scale? This can be addressed in the context of the most likely scenario in which Russia might attempt some incursion in NATO. In the book, *The Senkaku Paradox*, Michael O'Hanlon establishes some key scenarios that help define the most likely type of scenarios between great powers for armed conflict. Briefly,

---

[27] Ibid., p. 15.

[28] J. Kjellén, *Russian Electronic Warfare: The Role of Electronic Warfare in the Russian Armed Forces*, Swedish Defense Research Agency, FOI-R – 4625 – SE, September 2018.

[29] J. Kjellén, *A More Nuanced View of Russian Electronic Warfare*, Swedish Defense Research Agency, 6 March 2019.

[30] R. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging Russia in the Electromagnetic Spectrum*, International Centre for Defence and Security, Republic of Estonia Ministry of Defence, September 2017, p. 21.

[31] Ibid.

O'Hanlon's argument is that major military engagements between Russia and the US would be unlikely. The more likely scenario would be an incursion by the Russians in a small part of one of the Baltic states[32]. According to Roger McDermott, author of a detailed report on Russian EW capabilities: "If conflict with Russia ever erupts on NATO's Eastern Flank, the first sign of activity will be in the EMS – and in this spectrum the initiative and advantage will be determined"[33].

Electronic warfare is[34] a critical part of conflict throughout its stages, just as military command, control, communications and intelligence are. Prior to troop movements, artillery, missile and other physical attacks, EW is a precursor to hostilities. EW attacks have been performed by Russia in Crimea, Donbass, and Syria prior to and during physical hostilities. The recent Russian demonstration of GPS signal jamming during NATO's Trident Juncture exercises in northern Norway[35]. The EW attacks against GPS, which is a core technology associated with precision guided munitions (PGMs), may be an attempt to signal Russian willingness to try to neutralize one of NATO's key technological strengths. Or it may be simply a low-risk means to try to undermine NATO confidence in its capabilities. To ensure that NATO's command and control, precision-guided munitions, radar, and communications are demonstrably solid, there is no alternative than to engage in a concerted effort to maintain control of the electromagnetic environment.

It does not appear that Russia could make sudden strides in EW by applying modern AI algorithms. In the first place, modern AI algorithms are not easily substituted into the integrated, mature architectures of modern EW systems, as I have already argued. In the second place, Russia has not demonstrated the

---

[32] M.E. O'Hanlon, *The Senkaku Paradox: Risking Great Power War over Small Stakes*, Washington DC, Brookings Institution Press, Chapter 2, 2019.

[33] R. McDermott (2017), p. 28.

[34] Commander M. von Spreckelsen…, cit.

[35] B. Tigner, *Norway says Russia jammed GPS during major NATO exercise*, New Atlanticist/Atlantic Council, 15 November 2018.

investments in modern AI algorithms that the US and China have, and those two countries have not fielded AI-based EW systems. In the field of modern AI algorithm R&D, Russia has established a few innovation centers[36], and certainly starts from an historic tradition of strong advanced education and research in mathematics and related disciplines. However, Russia appears to have difficulty maintaining top talent[37], and there is has not been a long-term push from the very top for taking a leading role in modern AI algorithm development, in particular as compared with China's repeated emphasis over the past few years. Taking all this into account, there is unlikely to be a sudden, significant improvement in AI-enabled EW from Russia that would provide an overwhelming advantage to Russia in the electromagnetic spectrum[38]. More likely, Russia will continue to make progress in improving the responsiveness and speed of their EW systems.

[36] A. Bateman, "Russia's Quest to Lead the World in AI is Doomed", *Defense One*, 19 June 2019.

[37] Ibid.

[38] Although it is beyond the scope of this paper, I would argue for similar reasons that we are unlikely to see a sudden significant improvement in Russian command and control through the application of modern AI algorithms, as I define them here. The functions required in military command and control include: fusing data, estimating the locations, status, movements, etc. of hostile forces as well as own forces; forecasting this "tactical picture"; allocating resources optimally to counter threats; planning routes subject to tactical, environmental and physical constraints; and continually updating this process as new data arrives. Algorithmic solutions to this wide variety of tasks are similarly varied, and no single type of algorithm appears the best choice to integrate all these functions. Russian announcements of integrated command and control systems, (R. McDermott, "Moscow Showcases Breakthrough in Automated Command and Control", *Eurasia Daily Monitor*, vol. 16, no. 164, 20 November 2019) should be taken very seriously as advances in algorithms and integration, but not as evidence of AI breakthroughs per se.

Conclusion

We have seen that Russia has an interest in EW to protect its own forces and to disrupt its adversaries in military crises as well as full scale military operations, and has been investing and training its capabilities. It is not an EW superpower, and many of the Russian capabilities are defensive in nature. We have also seen that EW technology is inherently automated due to the rapid speed of signal generation, propagation, and processing. Advances in digital technology have made it possible for modern militaries to develop highly flexible and adaptable electronic systems with feedback that enable rapid adaptation to the electromagnetic environment. While modern AI algorithms are being applied to EW through research and development, there is no indication of any kind of breakthrough in the foreseeable future.

Russia will be capable of continuing developments in EW, and may introduce some elements of deep neural networks for signal recognition. However, Russia is unlikely to develop any kind of decisive lead in this area as long as the US and its NATO allies continue to invest in the EW countermeasures to the measures that are developed.

The temptation to disrupt communications over the internet as well as in the electromagnetic environment will remain a strong for Russia if it attempts further incursions. According to the National Defense Strategy Commission report:

> Electronic warfare capabilities will be critical in any future conflict, especially those against major-power rivals. U.S. competitors have invested heavily in electronic warfare as a way of neutralizing U.S. advantages and weakening America's ability to project power. Recommendation: DOD must enhance its electronic warfare capacity and capability to overcome adversary electronic warfare investments, and to degrade and defeat anti-access/area denial capabilities and adversary command, control, and communications architectures[39].

[39] National Defense Strategy Commission, *Providing for the Common Defense. The*

Finally, there is paradox of effective US/NATO electronic warfare capability that goes to the core of an extensive debate about modern AI algorithms and autonomous weapons. The ability of robust EW to control, deny, and even manipulate radio and other EM transmissions and sensors will interfere with human control over remote weapons. In a highly contested EW environment, human control over unmanned platforms, sensors, and in particular weapons becomes unreliable. This uncertainty will create a technological imperative for unmanned systems to become autonomous. Balancing the need for robust EW for warfighting, and avoiding a rapid drive toward lethal autonomy will be a complex debate.

Assessment and Recommendations of the National Defense Strategy Commission, 2018, p. 68.

5. Artificial Intelligence, Geopolitics, and Information Integrity

John Villasenor

Much has been written, and rightly so, about the potential that artificial intelligence (AI) can be used to create and promote misinformation. But there is a less well-recognized but equally important application for AI in helping to *detect* misinformation and limit its spread. This dual role will be particularly important in geopolitics, which is closely tied to how governments shape and react to public opinion both within and beyond their borders. And it is important for another reason as well: While nation-state interest in information is certainly not new, the incorporation of AI into the information ecosystem is set to accelerate as machine learning and related technologies experience continued advances.

The present article explores the intersection of AI and information integrity in the specific context of geopolitics. Before addressing that topic further, it is important to underscore that the geopolitical implications of AI go far beyond information. AI will reshape defense, manufacturing, trade, and many other geopolitically-relevant sectors. But information is unique because information flows determine what people know about their own country and the events within it, as well as what they know about events occurring on a global scale. And information flows are also critical inputs to government decisions

regarding defense, national security, and the promotion of economic growth. Thus, a full accounting of how AI will influence geopolitics of necessity requires engaging with its application in the information ecosystem.

This chapter begins with an exploration of some of the key factors that will shape the use of AI in future digital information technologies. It then considers how AI can be applied to both the creation and detection of misinformation. The final section addresses how AI will impact efforts by nation-states to promote – or impede – information integrity.

AI and the Information Ecosystem: Some Key Factors

Advancing AI Technologies

A combination of factors will determine how AI will impact the information ecosystem over the next decade. First, there is the technology itself. Spurred by extraordinary levels of both private and public investment, AI is advancing at far greater rates than in the past. According to CB Insights, venture capital investment in the United States in AI startups grew from $4.1 billion in 2016 to $5.4 billion in 2017 to $9.3 billion in 2018[1]. The US government has also been ramping up its support for AI research. For example, in fall 2018 the US Department of Defense's Defense Advanced Research Projects Agency (DARPA) announced a "$2 billion campaign to develop next wave of AI technologies"[2].

In China, which views AI as a central focus of its goal of becoming a technological superpower, the government has launched a wide array of multi-billion-dollar AI investment

[1] CB Insights, "VCs Nearly Doubled Their Investment in This Tech Last Year", 20 February 2019.

[2] Defense Advanced Research Project Agency, "DARPA Announces $2 Billion Campaign to Develop Next Wave of A.I. Technologies", 7 September 2018.

initiatives[3]. Israel is another key player in the global AI landscape. In 2018, "AI-related companies accounted for 17% of the total number of 6,673 active Israeli tech companies in Israel tracked by Start-Up Nation Finder" and "32% of all funding rounds and 37% of the total capital raised went to AI-related companies"[4]. And in Europe, the European Commission has announced a plan aimed at spurring "more than €20 billion per year from public and private investments" in AI over the 2020s[5].

An additional aspect of the landscape not captured by the statistics above is the enormous internal AI research and development investment being made by large companies such as Amazon, IBM, Google, and Microsoft. Collectively, the capital flowing from governments, venture investors, and corporations will spur extraordinary AI advances, greatly broadening the capacity to analyze and make effective use of data. Relatedly, continued investment will make AI better at learning, opening the door to increasingly sophisticated algorithms that combine human ingenuity with computer-driven insights.

The Growing Role of AI in the Digital Ecosystem

A second factor that will elevate the role of AI is the degree to which it will be increasingly intertwined with broader digital information ecosystem. Many of the most important information technology changes of the last quarter of a century – including the growth of the internet, advances in digital storage and computation capacity, and the introduction and mass adoption of smartphones and social media – have occurred largely (though not completely) without AI. By contrast, the future evolution of the digital information landscape will be driven in significant part by AI.

---

[3] T.H. Davenport, "China Is Executing its for AI while is still wrestling to create one", *Market Watch*, 27 February 2019.

[4] A. Mizroch, "In Israel, A Stand Out Year for Artificial Intelligence Technologies", *Forbes*, 11 March 2019.

[5] AI Europe Hub, "European Union to Invest 20 Billion Euros in AI".

Over about the last five years, we have been experiencing the first stages of this transition, and AI is now used a wide range of commercial products and services. There is an understandable temptation to predict the future by extrapolating the past, and therefore to conclude that the next 5 or 10 years see the introduction of even more AI into the commercial ecosystem to enhance consumer services in areas such as transportation, online purchasing, and media delivery. But while that prediction is no doubt accurate, it almost certainly fails to anticipate the more profound AI-induced changes that are much harder to foresee in advance.

By analogy, consider the internet in the late 1990s. At that time, it would have been relatively easy to predict dramatic growth in both the number and diversity of web sites over the subsequent 10 years. But it would have been much harder to envision the growth and impact of social media—which we now know spurred far more significant changes than did growth in the number of websites. In the same way, it is easy today to conclude that AI will play an increasingly large role in the digital information landscape over the next decade, but far harder to anticipate its use in ways that lack clear historical antecedents.

Information Gatekeepers

Information gatekeepers, including but not limited to social media companies, constitute a third factor influencing how AI will shape the information ecosystem. For large-scale social media companies, as well as other companies (such as online retailers and providers of internet and mobile phone services) that engage with millions of individual users, the question is not whether to incorporate AI, but rather how it should be most effectively used to further goals such as offering highly customized content to consumers and detecting fraud. As AI continues to advance, companies seeking to take advantage of the cost efficiencies it enables have incentives to deploy it more extensively in their systems. Companies will make highly

consequential policy choices regarding their development and rollout of AI solutions, addressing questions such as the extent to which they should curate and/or filter content, the standards they will apply in relation to testing and monitoring algorithms to detect problems such as bias, and the level of human oversight to provide in relation algorithmic decisions and algorithmic evolution.

In authoritarian countries, an additional information gatekeeper is the government itself. All authoritarian governments will seek to use AI to monitor online traffic and detect digital content deemed problematic. But there will be variations both across and within authoritarian countries in the nature of the tools employed and the extent to which they are used to actively control (as opposed to monitor) discourse.

AI and Information Integrity

"Information integrity" as used herein is intended to describe the extent to which information is accurate, non-deceptive, and properly attributed. While accuracy is clearly a baseline requirement to achieve information integrity, accuracy alone will not always be sufficient. For information to have integrity it also has to be contextualized in a manner that avoids deception. To take a simple example, consider a politician who accompanies a family member who has struggled with drug addiction on a visit to a drug rehabilitation clinic. Suppose that the politician is photographed when leaving the clinic, and that those photographs are then distributed on social media. The photographs are accurate in the sense of depicting an event that actually occurred, but they are deceptive because, when distributed without context, they could imply that the politician is personally struggling with drug addiction.

Attribution is also important. A social media posting purporting to come from a voter and containing accurate, properly contextualized content still lacks integrity if in fact it was posted by a foreign government aiming to influence an election. Thus,

challenges to assessing the integrity of information include not only evaluating truth or falsity, but also identifying the extent to which decontextualization may lead to misinterpretation, as well as understanding whether the purported source is the same as the actual source.

Much of the recent public dialog regarding the role of AI in information integrity has focused on potential negative impacts. Deepfakes, which are videos produced with the aid of deep learning techniques that portray people doing or saying things that they never did or said, have been correctly identified as a major potential concern[6]. A well-constructed deepfake targeting a politician, if released onto the internet at the right time and manner, could potentially swing a close election.

AI can also be used to undermine information integrity in other ways. Consider "bots", which describe accounts on Twitter and other social media platforms that masquerade as humans but are actually software (though as of yet, not generally *AI-enabled* software). While precise statistics on the percentage of Twitter accounts that are bots are hard to come by (in part due to fluctuations over time as different bot detection techniques are developed and deployed, and as bot creators then react by updating their methods), it is clear that the number is very high.

Bots are known to play an important role in amplifying online misinformation. A November 2018 paper published in *Nature Communications* reported on a study of "14 million messages spreading 400 thousand articles on Twitter during ten months in 2016 and 2017"[7]. The authors found "evidence that social bots played a disproportionate role in spreading articles from low-credibility sources. Bots amplify such content in the early spreading moments, before an article goes viral. They also

[6] It is important to note that deepfakes are not inherently bad. Deepfakes have plenty of innocuous uses as well, including in areas such as education and entertainment.

[7] C. Shao et al., "The spread of low-credibility content by social bots", *Nature*, vol. 9, 2018.

target users with many followers through replies and mentions. Humans are vulnerable to this manipulation, resharing content posted by bots"[8]. As noted above, in the past, most bots have not been AI-enabled. Inevitably, this will change. Well-designed AI-powered bots could do a very effective job of impersonating humans, making them much harder to detect and more effective at disseminating misinformation.

As concerning as the above examples are, it is also important to consider the other side of the ledger. Just as AI can be used to promote misinformation, it can also be used to combat it. Deepfake detection is one example. There is a very active community of researchers working to develop methods, including approaches based on AI, to automatically identify manipulated videos. Examples include the use of deep learning to identify artifacts introduced by face-swapping software[9] and the use of neural networks to identify frame-to-frame inconsistencies in deepfake videos[10]. As a February 2019 article in *IEEE Spectrum* noted, "the AI Foundation raised $10 million to build a tool that uses both human moderators and machine learning to identify deceptive malicious content such as deepfakes"[11]. The same article also described efforts by a Netherlands-based technology startup to use adversarial machine learning "as a primary tool for detecting deepfakes"[12].

AI can also be used to detect activity by bots. Bots that do not rely on AI often act in recognizable ways that can easily be detected. The authors of the *Nature Communications* article noted above observed that when low-credibility content goes viral, it exhibits "distinctive patterns"[13]. The authors explained that

---

[8] Ibid.

[9] Yuezun Li and Siwei Liu, *Exposing DeepFake Videos by Detecting Face Warping Artifacts*, Working Paper, 22 May 2019.

[10] D. Guera and E.J. Delp, *Deefake Video Detection Using Recurrent Neural Networks*, Working Paper.

[11] J. Hsu, *Can AI Detect DeepFakes to Help Ensure Integrity of U.S. 2020 Elections*, IEEE, 28 February 2019.

[12] Ibid.

[13] C. Shao et al. (2018).

> most articles by low-credibility sources spread through original tweets and retweets, while few are shared in replies; this is different from articles by fact-checking sources, which are shared mainly via retweets but also replies. In other words, the spreading patterns of low-credibility content are less "conversational". Second, the more a story was tweeted, the more the tweets were concentrated in the hands of few accounts, who act as "super-spreaders"[14].

By contrast, in the future when many bots become AI-enabled, they will be more capable of emulating organic, non-coordinated viral behavior, in part by creating larger networks to spread tweets and in part by relying more on including misinformation in "replies" that might appear to have been written by a real person. The most effective way to identify and block AI-enabled bots will be to use AI in the detection algorithms. Such algorithms could monitor the evolving behavior of a bot network, and in response evolve their own templates for identifying likely non-human social media activity.

The examples of deepfakes and bots illustrate that while misinformation poses major challenges, the same powerful AI techniques that can be employed to produce false or deceptive content can also be applied to its detection and mitigation. A challenge is that the asymmetries involved give misinformation creators an inherent set of advantages. They can continually enhance their algorithms to stay one step ahead of the latest detection techniques. And, to have impact, misinformation creators only have to succeed some of the time. Even if only a low percentage of malicious content evades detection, that can still be enough to cause significant harms.

Governments and the Information Ecosystem

As the above discussion makes clear, over the next decade AI will experience dramatic advances and take on an increasing role in the broader digital information ecosystem. At the same

[14] Ibid.

time, AI-based techniques for generating misinformation will become more sophisticated, as will techniques for detecting and impeding its spread.

This will impact geopolitics in multiple important ways. In authoritarian countries, governments have always sought to exert high levels of control over information, both through propagation of state-approved content and censorship of content deemed inconsistent with the government objectives. AI offers a powerful tool for achieving these ends. To take one example, AI can make it easy for an authoritarian country to perform highly detailed inspection and censorship of social media postings. Postings can be examined not only individually, but also in the aggregate for an individual or group of individuals to identify broader trends that might be of interest to the government. Authoritarian governments will make use of these capabilities to further geopolitical (and other) goals.

Inevitably, some governments will also seek to use online misinformation to alter elections in other countries. The well-documented foreign manipulation of US social media to attempt to influence the 2016 US presidential election is, unfortunately, only a foreshadowing of what is likely to occur in future high-stakes elections. AI-powered misinformation aimed at swaying voter perceptions can be very effective. Combating it will be challenging in part because of the high degree of coordination that would be needed among multiple private and public sector entities to identify and mitigate foreign government misinformation. Yet another complicating factor is that some forms of manipulation can be subtle and therefore not easily detectable. For instance, a foreign government might use AI to create social media accounts in the target country and cause those accounts to engage in much more humanlike behavior than would be possible without AI. The accounts could be used not only to propagate outright misinformation, but also to amplify negative but accurate information about a political candidate, thereby giving it more visibility among the electorate than it would have received absent the foreign influence.

A foreign government seeking to tip the scales in an election would have a long list of options for specific ways of undermining information integrity. A 2019 RAND Corporation report on "Hostile Social Manipulation" identifies over a dozen methods of social manipulation, including "content creation", "disinformation", "social media commenting", "direct advertising", "trolling", "behavioral redirection" and "microtargeting"[15]. With AI, all of these methods could be used at scale and in ways that might be difficult to mitigate, particularly given the importance of minimizing false positives, which could lead to suppression of legitimate social media content posted by real voters.

While election interference is an extremely important way in which nation-state might seek to use AI-generated misinformation to further geopolitical goals, it is not the only one. Nation-states might also use AI to disseminate information aimed at influencing a foreign government's geopolitically-relevant legislation; regulations; trade, economic, and defense policies; and decisions regarding major mergers and acquisitions. A nation state might also manipulate information to boost positive consumer perceptions of companies headquartered within the nation-state, thereby boosting the global competitiveness of those companies, and by extension, the nation-state. And, AI-enabled information manipulation will be a central feature of any future large-scale military conflict. This would include not only attempts to shape public opinion, but also efforts to undermine the availability and accuracy of information relied upon by military decisionmakers and political leaders.

Conclusion

So how can societies – and in particular democracies built on the free flow of information and ideas – address AI-enabled misinformation created and/or propagated by a foreign government?

[15] M.J. Mazarr et al., Hostile Social Manipulation, RAND, 2019.

Technology, policies, and awareness can all contribute to a solution. With respect to technology, as noted above, the same advances in AI that are making it easier to generate misinformation can also be used to detect it. Many of the tradeoffs involved parallel those found in cybersecurity, where there are also complex decisions to be made regarding how to allocate resources in relation to prevention, detection, and mitigation. The experience from that sector can help inform both public and private sector approaches to ensuring information integrity.

Governments should be both investing directly in research on improved detection as well serving as a resource for the private sector through information-sharing arrangements that can help companies better understand potential foreign manipulation of social media and other online information. The information flow can work in the other direction as well: Companies, and in particular social media companies, will be at the front lines of foreign-directed misinformation campaigns, and thus are well positioned to understand their dynamics and convey the lessons learned on to other companies and to the government.

Policy solutions can include the use of existing legal frameworks as well as new legislation. In considering the legal landscape, it is important to keep in mind that not all approaches that undermine information integrity will involve false statements. A foreign government might simply seek to amplify or suppress accurate information in ways aimed at swaying public opinion. When this occurs in the context of an election, it can be addressed through statutes aimed at combating election meddling. As important as such statutes are, their effectiveness will be limited due to the time scales involved (in many cases, the election will be long over by the time the legal system swings into action) and due to the fact that elections represent only one of the many potential targets of a misinformation campaign.

That highlights the importance of a final tool: increased awareness. In an era where deepfakes and other forms of manufactured or manipulated content will become more common,

broader awareness can help slow (though certainly not stop) their spread. In promoting this greater understanding, it will also be important not to undermine the trust in legitimate information which is at the foundation of all democratic societies.

6. Norms and Strategies for Stability in Cyberspace

Mariarosaria Taddeo

Cyber attacks are becoming more frequent and impactful. Each day in 2017, the United States suffered, on average, more than 4,000 ransomware attacks, which encrypt computer files until the owner pays to release them. In 2015, the daily average was just 1,000. In May 2017, when the WannaCry virus crippled hundreds of IT systems across the UK National Health Service, more than 19,000 appointments were cancelled. A month later, the NotPetya ransomware cost pharmaceutical giant Merck, shipping firm Maersk, and logistics company FedEx around $300 m each. Estimates show that global damages from cyber attacks may reach $6 tn a year by 2021[1].

The fast-pace escalation of cyber attacks occurred during the past decade has prompted a mounting concern about international stability and the security of our societies. To address this concern, in April 2017, the foreign ministers of the G7 countries approved a "Declaration on Responsible States Behaviour in Cyberspace"[2] (G7 Declaration 2017). In the opening statement, the G7 ministers stress their concern

[1] Herjavec Group, 2017 Cybercrime Report, Cybersecurity Ventures, 2017. Inside the Cunning, Unprecedented Hack of Ukraine's, Power Grid

[2] G7 Declaration 2017, "G7 Declaration on Responsible State Behavior in Cyberspace", Lucca, 2017, p. 1.

> […] about the risk of escalation and retaliation in cyberspace […]. Such activities could have a destabilizing effect on international peace and security. We stress that the risk of interstate conflict as a result of ICT incidents has emerged as a pressing issue for consideration. […], (G7 Declaration 2017, 1)[3].

Paradoxically, state actors often play a central role in the escalation of cyber attacks. State-run cyber attacks have been launched for espionage and sabotage purposes since 2003. Well-known examples include Titan Rain (2003), the Russian attack against Estonia (2006) and Georgia (2008), Red October targeting mostly Russia and Eastern European Countries (2007), Stuxnet and Operation Olympic Game against Iran (2006-2012). In 2016, a new wave of state-run (or state-sponsored) cyber attacks ranged from the Russian attack against Ukraine power plant[4], to the Chinese and Russian infiltrations US Federal Offices[5], to the Shamoon/Greenbag attacks on government infrastructures in Saudi Arabia[6]. WannaCry has been attributed to North Korea and NotPetya to Russia in 21017. Russia has also been linked to a series of cyber attacks targeting US critical national infrastructures disclosed in 2018.

This trend will continue. The relatively low entry-cost and the high chances of success mean that states will keep developing, relying on, and deploying cyber attacks. At the same time, the Artificial Intelligence (AI) leap of cyber capabilities – the use of AI technologies for cyber offence and defence – indicates that cyber attacks will escalate in frequency, impact, and sophistication[7].

---

[3] Ibid.

[4] "Inside the Cunning, Unprecedented Hack of Ukraine's, Power Grid", *Wired.com*, 3 March 2016.

[5] "The Perfect Weapon: How Russian Cyberpower Inveded the U.S.", *The Washington Post*, 13 December 2016.

[6] "Greenbug cyberespionage group targeting Middle East, possible links to Shamoon", Symantec Official Blog, 23 January 2017.

[7] L. Floridi and M. Taddeo, "Regulate Artificial Intelligence to Avert Cyber Arms Race", *Nature*, vol. 556, no. 7701, 2018a, pp. 296-98.

Cyber attacks contribute to shape political relations, national, and international equilibria of our societies and are becoming a structural element of their power dynamics. For this reason, it is crucial to identify and define *regulations* for state behaviour and *strategies* to deploy countering measures that would avoid escalation and disproportionate use of cyber means, while protecting and fostering the stability of our societies.

Regulations and strategies will only be effective insofar as they will rest on a deep understanding of the nature of these attacks, of their differences from violent (kinetic) ones, as well as on a clear understanding of the moral principles that should shape state behaviour in cyberspace. In the first part of this chapter, I will analyse existing approaches to the regulation of state behaviour in cyberspace and to the specification of deterrence strategies as countering strategies. This analysis will provide the groundwork for the theory of cyber deterrence and for the policy recommendations that I offer in the second part of the chapter.

Analogies and Regulation

Efforts to regulate state-run (or sponsored) cyber attacks – and cyber conflicts understood as attack-and-response dynamics – rose to prominence almost a decade ago, when the risks for national and international security and stability arising from the cyber domain became clear[8]. As I argued elsewhere[9], these efforts often rely on an *analogy-based approach*, according to which the regulatory problems concerning cyber attacks are only apparent, insofar as these are not radically different from other kinetic of attacks. Those endorsing this approach claim that the existing legal framework governing inter-state, kinetic attacks is sufficient to regulate cyber attacks, and by extension cyber conflicts. All that is needed is an in-depth analysis of such laws and an adequate interpretation of the phenomena, as there is

[8] http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

[9] M., Taddeo, "Just Information Warfare", *Topoi*, 1-12 April 2014.

> a thick web of international law norms suffuses cyber-space. These norms both outlaw many malevolent cyber-operations and allow states to mount robust responses[10].

According to this view, interpretations often highlight that existing norms raise substantial barriers to the use of cyber weapons and to the use of force to defend cyberspace; and international law contains coercive means of permitting lawful responses to cyber provocations and threats of any kind. The legal framework that is referred to encompasses the four Geneva Conventions and their first two Additional Protocols, the international customary law and general principle of law, the Convention restricting or prohibiting the use of certain conventional weapons, and judicial decisions. Arms control treaties, such as the Nuclear Non-Proliferation Treaty and the Chemical Weapons Convention, are often mentioned as providing guidance for action in the case of kinetic cyber attacks[11]. At the same time, coercive measures addressing economic violations are generally considered legitimate in the case of cyber attacks that do not cause physical damage[12].

Others maintain that the problem at stake is not whether cyber attacks and cyber conflicts can be interpreted in such a way as to fit the parameters of kinetic conflicts, economic transgressions, and conventional warfare, and hence whether they fall within the domain of international humanitarian law, as we know it. The problem rests at a deeper level and questions the very normative and conceptual framework of international humanitarian law and its ability to address *satisfactorily* and *fairly* the changes prompted by cyber conflicts[13].

---

[10] M. Schmitt, "Cyberspace and International Law: The Penumbral Mist of Uncertainty", *Harvard*, vol. 126, no. 176, 2013, 176-80, p. 177.

[11] Ibid.

[12] H. Lin, "Cyber Conflict and International Humanitarian Law", *International Review of the Red Cross*, vol. 94, no. 886, 2012, pp. 515-31; M.E. O'Connell, "Cyber Security without Cyber War", *Journal of Conflict and Security Law*, vol. 17, no. 2, pp. 187-209, 2012.

[13] R. Dipert, "Ethics of Cyberwarfare", *Journal of Military Ethics*, vol. 9, no. 4, pp.

Consider for example inter-state cyber conflicts. Regulation of these conflicts need to be developed consistently to (a) Just War Theory, (b) human rights, and (c) international humanitarian laws. However, applying (a)-(c) to the case of cyber conflicts proves to be problematic given the changes in military affairs that they prompted[14]. When compared to kinetic ones, cyber conflicts show fundamental differences: their domain ranges from the virtual to the physical; the nature of their actors and targets involves artificial and virtual entities alongside human beings and physical objects; and their level of violence may range from non-violent to potentially highly violent phenomena. These differences are redefining our understanding of key concepts such as harm, violence, target, combatants, weapons, and attack, and pose serious challenges to any attempt to regulate conflicts in cyberspace[15].

Things are not less problematic when considering ethical issues. Cyber conflicts bring about three sets of problems, concerning risks, rights, and responsibilities (3R problems)[16]. The more contemporary societies are dependent on digital technologies, the more the 3R problems become pressing and undermine ethically blind attempts to regulate cyber conflicts. Consider the risks of escalation. Estimates indicate that the cyber security market will grow from $106 billion in 2015 to $170 billion by 2020, posing the risk of a progressive weaponization and militarization of cyberspace[17]. At the same time, the reliance on malware for

384-410, 2010; L. Floridi and M. Taddeo (eds.), *The Ethics of Information Warfare*, New York, Springer; M. Taddeo (2014a).

[14] R. Dipert (2010); M. Taddeo, "An Analysis for a Just Cyber Warfare", in "4th International Conference on Cyber Conflict" (CYCON 2012), pp. 1-10; L. Floridi and M. Taddeo (2014).

[15] R. Dipert (2010); M. Taddeo, "Information Warfare: A Philosophical Perspective", *Philosophy and Technology*, vol. 25, no. 1, 2012b, pp. 105-20; R. Taddeo (2014a); L. Floridi and M. Taddeo (2014a); M. Taddeo, "The Struggle Between Liberties and Authorities in the Information Age", *Science and Engineering Ethics*, September, 2014b, pp. 1-14.

[16] M. Taddeo (2012a).

[17] L. Floridi and M. Taddeo (2018a), pp. 296-98.

state-run cyber operations (like Titan Rain, Red October, and Stuxnet) risks sparking a cyber arms race and competition for digital supremacy, hence increasing the possibility of escalation and conflicts[18]. Regulations of cyber conflicts need to address and reduce this risk by encompassing principles to foster cyber stability, trust, and transparency among states[19]. At the same time, cyber threats are pervasive. They can target, but can also be launched through, civilian infrastructures, e.g. civilian computers and websites. This may (and in some cases already has) initiate policies of higher levels of control, enforced by governments in order to detect and deter possible threats. In these circumstances, individual rights, such as privacy and anonymity may come under sharp, devaluating pressure[20].

Ascribing responsibilities also prove to be problematic when considering cyber attacks. Cyberspace affords a certain level of anonymity, often exploited by states or state-sponsored groups and non-state actors. Difficulties in attributing attacks allow perpetrators to deny responsibility, and pose an escalatory risk in cases of erroneous attribution. The international community faced this risk in 2014, when malware initially assessed as capable of destroying the content of the entire stock exchange was discovered on Nasdaq's central servers and allegations were made of a Russian origin for the software[21].

---

[18] MarketsandMarkets, "Cyber Security Market by Solutions & Services - 2020", 2015.

[19] J. Arquilla and D.A. Borer, *Information Strategy and Warfare : A Guide to Theory and Practice*, New York, Routledge, 2007; U. Steinhoff, " On the Ethics of War and Terrorism", Oxford-New York, Oxford University Press, 2007; European Union, "Cyber Diplomacy: Confidence-Building Measures - Think Tank", Brussels, 2015; M. Taddeo, "An Analysis For A Just Cyber Warfare", in Fourth International Conference of Cyber Conflict, NATO CCD COE and IEEE Publication, forthcoming.

[20] J. Arquilla, "Ethics and Information Warfare", in Z. Khalilzad and J.P. White (eds.), *Strategic Appraisal: The Changing Role of Information in Warfare*, Santa Monica, CA, RAND, pp. 379-401, 1999; D.E. Denning. "The Ethics of Cyber Conflict", in K.E. Himma and H.T. Tavani (eds.), *Information and Computer Ethics*, Hoboken, USA, Wiley, 2007; M. Taddeo, "Cyber Security and Individual Rights, Striking the Right Balance", *Philosophy & Technology*, vol. 26, no. 4, pp. 2013, pp. 353-56.

[21] D. Goodin, "How elite hackers (almost) stole the NASDAQ", *ArsTechnica*, 17

In the medium- and long-term, regulations need to be defined so to ensure security and stability of societies, and avoid risks of escalation. To achieve this end, efforts to regulate state-run cyber attacks will have to rely on an in-depth understanding of this new phenomenon; identify the changes brought about by cyber warfare and the information revolution[22]; and define a set of shared values that will guide the different actors operating in the international arena. The alternative is developing unsatisfactory, short-sighted approaches and facing the risk of a cyber backlash: a deceleration of the digitization process imposed by governments and international institutions to prevent this kind of conflicts to erode both the trust in economy and in political institutions. For this reason, it is necessary to seize the limits of the analogy-based approach, and to move past it. As Betz and Stevens put it:

> It is little wonder that we attempt to classify […] the unfamiliar present and unknowable future in terms of a more familiar past, but we should remain mindful of the limitations of analogical reasoning in cyber security[23].

Analogies can be powerful, for they inform the way in which we think and constrain ideas and reasoning within a conceptual space[24]. However, if the conceptual space is not the right one, analogies become misleading and detrimental for any attempt to develop innovative and in-depth understanding of new

---

July 2014.

[22] L. Floridi, *The Fourth Revolution, How the Infosphere Is Reshaping Human Reality*, Oxford, Oxford University Press, 2014; M. Taddeo and E. Buchanan, "Information Societies, Ethical Enquiries", *Philosophy & Technology*, vol. 28, no. 1, 2015, pp. 5-10. L. Floridi and M. Taddeo, "What Is Data Ethics?", *Philosophical Transactions of the Royal Society A. Mathematical, Physical and Engineering Sciences*, vol. 374, no. 2083, 2016.

[23] D.J. Betz and T. Stevens, "Analogical Reasoning and Cyber Security", *Security Dialogue*, vol. 44, no. 2, 2013, pp. 147-64.

[24] L. Wittgenstein, *Philosophical investigations*, Rev. 4th ed. Chichester, West Sussex, UK , Malden, MA, Wiley-Blackwell, 2009.

phenomena, and they should be abandoned altogether. When the conceptual space is the right one, analogies are at best a step on Wittgenstein's ladder and need to be disregarded once they have taken us to the next level of the analysis. This is the case of the analogies between kinetic and cyber conflicts.

Cyberspace and cyber conflicts are now *relatively* new phenomena. Over the past two decades, possible uses, misuses, risks, and affordances of both have become clearer. As societies, we now know the successes, the failures, and the lessons learned necessary to start analysing and understanding the nature of cyberspace and cyber conflicts and to regulate appropriately both the environment and the actions in it to avoid risks of escalation and instability.

The Strategic Nature of Cyberspace

Escalation follows from the nature of cyber attacks and the dynamics of cyberspace[25]. Non-kinetic cyber attacks – aggressive uses of information and communications technologies that do not cause destruction or casualties, e.g. deploy zero-day exploits or DDoS attacks – cost little in terms of resources and risks to the attackers, while having high chances to be successful. At the same time, cyber defence is porous by its own nature[26]: every system has bugs in the program (vulnerabilities), identifying and exploiting them is just a matter of time, means, and determination. This makes even the most sophisticate cyber defence mechanisms ephemeral and, thus, limits their potential to deter new attacks.

[25] L. Floridi and M Taddeo (2014a); M. Taddeo (2014a); M. Taddeo, "On the Risks of Relying on Analogies to Understand Cyber Conflicts", *Minds and Machines*, vol. 26, no. 4, 2016, pp. 317-21; M. Taddeo, "Cyber Conflicts and Political Power in Information Societies", *Minds and Machines*, vol. 27, no. 2, 2017, pp. 265-68.

[26] P.M. Morgan, "The State of Deterrence in International Politics Today", *Contemporary Security Policy*, vol. 33, no. 1, 2012, pp. 85-107.

Even when successful, cyber defence does not lead to strategic advantages, insofar as dismounting a cyber attack, may bring tactical success, but very rarely leads to the ultimate defeating of an adversary[27]. This creates an environment of *persistent offence*[28], where attacking is tactically and strategically more advantageous than defending. As Haknett and Goldman argue, in an offence-persistent environment, defence can achieve tactical and operational success in the short term if it can adjust constantly to the means of attack, but it cannot win strategically. Offence will persist and the interactions with the enemy will remain constant. This is why inter-state cyber defence have shifted from reactive (defending) towards an *active* (countering) defence strategies.

In this scenario, state actors make policy decisions to protect their abilities to launch cyber attacks. *Strategic ambiguity* is one of these decisions. According to this policy, states decide neither to define and nor inform the international community about their *red lines* – thresholds that once crossed would trigger state response – for non-kinetic cyber attacks[29]. This approach leaves *de facto* unregulated cyber attacks that remain below the threshold of an armed attack.

Strategic ambiguity has often been presented as a way to confuse the opponents about the consequences of their cyber attacks. As the US National Intelligence Officer for Cyber Issues officer put it:

> Currently most countries, including ours, don't want to be incredibly specific about the red lines for two reasons: You don't want to invite people to do anything they want below that red line thinking they'll be able to do it with impunity, and secondly, you don't want to back yourself into a strategic corner where you have to respond if they do something above that red line or else lose credibility in a geopolitical sense[30].

---

[27] M. Taddeo (2017).

[28] R.J. Harknett and E.O. Goldman, "The Search for Cyber Fundamental", *Journal of Information Warfare*, vol. 15, no. 2, 2016, pp. 81-88.

[29] M. Taddeo, "Information Warfare: A Philosophical Perspective", *Philosophy & Technology*, vol. 25, no. 1, 2011, pp. 105-20.

[30] M. Pomerleau, *Cyber red lines: ambiguous by necessity?*, C4ISRNET, 8 September

However, by fostering ambiguity, state actors also leave open for themselves a wider room for manoeuvring. Strategic ambiguity allows state actors to deploy cyber attacks for military, espionage, sabotage, and surveillance purposes without being constrained by their own policies or international red lines. This makes ambiguity a dangerous choice, one that is strategically risky and politically misleading.

The risks come with the cascade effect following the absence of clear thresholds for cyber attacks. The lack of thresholds facilitates a proliferation of offensive strategies. This, in turn, favours an international cyber arms race and the weaponization of cyberspace, which ultimately spurs the escalation of cyber attacks. This is why strategic ambiguity is a policy hazard that fuels, rather than arrest, escalation of interstate cyber attacks. Cyber attacks would be deterred more effectively by a regime of international norms that makes attacks politically costly to the point of being disadvantageous for the state actors who launch them.

As I mention in section 1, stability of cyberspace hinges on both regulations and strategies. Having considered the limits of the existing approaches to the regulation of state behaviour in cyberspace, I shall now focus on existing view for the designing deterrence strategies for cyber attacks.

Conventional Deterrence Theory

Concerned by the risks of escalation, international organizations such as NATO, the UN Institute for Disarmament Research (UNIDIR), and national governments, like the UK and US have started to consider whether, and how to, deploy deterrence to foster stability of cyberspace.

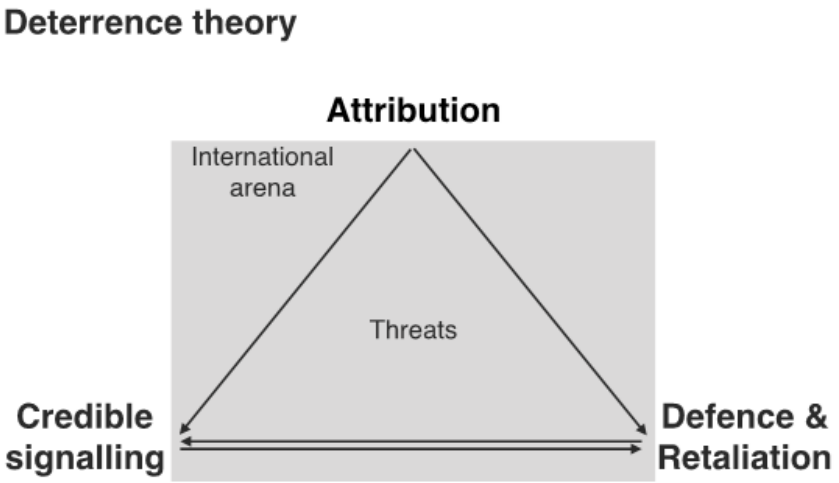
However, deploying cyber deterrence strategies is challenging. For conventional deterrence theory (hereafter: deterrence theory) does not work in cyberspace, as it does not address the global reach, anonymity, the distributed, and interconnected

---

2018.

nature of this domain. Deterrence theory has three core elements: attribution of attacks; defence and retaliation as types of deterring strategies; and the capability of the defender to signal credible threats (see Figure 1). None of these elements is attainable in cyberspace.

Fig. 6.1 - The core elements of deterrence theory and their dependences



This figure was published in M. Taddeo., "The Limits of Deterrence Theory in Cyberspace", *Philosophy & Technology*, 2017

Consider attribution first. Prompt, positive attribution is crucial to deterrence: the less immediate is attribution, the less severe will be the defender's response. The less positive the attribution, the more time will be necessary to respond. In cyberspace, attribution is at best problematic, if not impossible. Cyber attacks are often launched in different stages and involve globally distributed networks of machines, as well as pieces of code that combine different elements provided (or stolen) by a number of actors. In this scenario, identifying the malware,

the network of infected machines, or even the country of origin of the attack is not sufficient for attribution, as attackers can design and route their operations through third-party machines and countries with the goal of obscuring or misdirecting attribution. The limits of attribution in cyberspace pose serious obstacles to the deployment of effective deterrence. Recalling Figure 1, without attribution defence and retaliation, as well as signalling, are left without a target and are undermined by the inability of the defender to identify the attacker.

Signalling credible threats is also problematic in cyberspace. This element hinges on state's reputation. In kinetic scenarios, reputation is gained by showcasing military capabilities and by showing ability to resolve (to deter or defeat the opponent) over time. To some extent, the same also holds true in cyberspace, where a state's reputation also refers to a state's past interactions in this domain, its known cyber capabilities to defend and offend, as well as its overall reputation in resolving conflicts. However, state's reputation in cyberspace may not necessarily correspond to actual capabilities in this domain, as states are reluctant to circulate information about the attacks that they receive, especially those that they could not avert. This makes signalling less credible and, thus, more problematic than in other domains of warfare.

Also conventional deterrence strategies, defence and retaliation, are problematic in cyberspace. Every system has its security vulnerabilities and identifying and exploiting them is simply a matter of time, means, and determination. This makes vulnerable even the most sophisticated defence mechanisms, thus limiting their potential to deter new attacks by defence. Unlikely deterrence by defence, deterrence by retaliation may be effective in cyberspace. However, this strategy is coupled with serious risk of escalation. This is because the means to retaliate, i.e. cyber weapons, are *malleable* and difficult to control. Cyber weapons can be accessed, stored, combined, repurposed, and redeployed much more easily than it was ever possible with other kinds of military capability. This was the case for example

of Stuxnet. Despite being designed to target specific configuration requirements of Siemens software installed on Iranian nuclear centrifuges, the worm was eventually released on the Internet and infected systems in Azerbaijan, Indonesia, India, Pakistan, and the US.

Clearly, classic deterrence theory faces severe limitations when applied in cyberspace. But it would be a mistake to conclude that as classic deterrence theory does not work in cyberspace, then deterrence is unattainable in this domain. As USN Commander Bebber stated:

> History suggests that applying the wrong operational framework to an emerging strategic environment is a recipe for failure. During the World War I, both sides failed to realize that large scale artillery barrages followed by massed infantry assaults were hopeless on a battlefield that strongly favored well-entrenched defense supported by machine gun technology. […] The failure to adapt had disastrous consequences[31].

We need to adapt. And adapting will be successful only if it rests on an in-depth understanding of cyberspace, cyber conflicts, their nature, and their dynamics. This understanding will allow us to forge a new theory of deterrence, one able to address the specificities of cyberspace and cyber conflicts. The alternative – developing cyber deterrence in analogy with conventional deterrence – is recipe for failure. It is equivalent to force the proverbial square peg in the round whole, we are more likely to smash the toy than to win the game.

Cyber Deterrence Theory

Cyber attacks and defence evolve with digital technology. As the latter becomes more autonomous and smart, leveraging the potential of AI, so do cyber attacks and cyber defence strategies.

[31] Commander Robert "Jake" Bebber, "There is No Such Thing as Cyber Deterrence. Please Stop", *The Cipher Brief*, 1 April 2018.

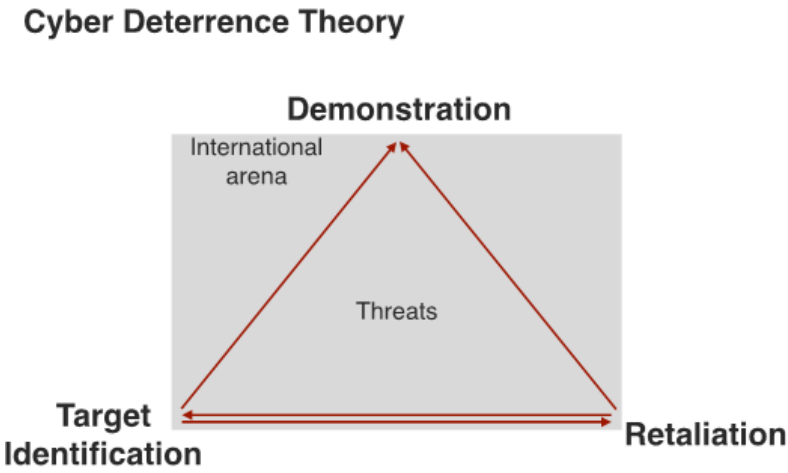
Both the public and private sectors are already testing AI systems in autonomous war games. The 2016, DARPA Cyber Grand Challenge was a landmark in this respect. The Challenge was the first, fully autonomous competition in which AI capabilities for defence were successfully tested. Seven AI systems, developed by teams from the United States and Switzerland, fought against each other to identify and patch their own vulnerabilities, while probing and exploiting those of other systems. The Challenge showed that AI will have a major impact on the waging of cyber conflicts, it will provide new capabilities for defence, shape new strategies, but also pose new risks. The latters are of particular concern. The autonomy AI systems, their capacity to improve their own strategies and launch increasingly aggressive counter-attacks with each iteration may lead to proportionality breaches and escalation of responses, which could, in turn, trigger kinetic conflicts. In this scenario, cyber deterrence is ever more necessary.

Elsewhere I argued that cyber deterrence rests on three core elements: target identification, retaliation, and demonstration (Figure 2)[32].

Target identification is essential for deterrence. It allows the defendant to isolate (and counter-attack) enemy systems independently from the identification of the actors behind them, thus side-stepping the attribution problem, while identifying a justifiable target for retaliation. Identifying the attacking system and retaliate is feasible task, one which AI systems for defence can already achieve. As shown in Figure 2, cyber deterrence does not encompass defence among its possible strategies. This is due to the offence persistent nature of cyberspace, which makes retaliation more effective than defence both tactically and strategically.

[32] M. Taddeo, "How to Deter in Cyberspace", *The European Centre of Excellence for Countering Hybrid Threats*, vol. 6, 2018, pp. 1-10.

Fig. 6.2 - The three elements of Cyber Deterrence Theory and their dependencies



M. Taddeo, "How to Deter in Cyberspace", *The European Centre of Excellence for Countering Hybrid Threats*, vol. 6, 2018, pp. 1-10.

Cyber deterrence uses target identification and retaliation for demonstrative purposes. According to this theory, deterrence in cyberspace works if it can demonstrate the defendant's capability to retaliate a current attack by harming the source system. While not being able to deter an incoming cyber attack, retaliation will deter the *next* round of attacks coming from the same opponent. This is because the mere threat of retaliation will not be sufficient to change the opponent's intentions to attacks. The chances of success and the likelihood that the attack will remain unattributed remain too high for any proportionate threat to be effective. Thus, to be successful, cyber deterrence need to shift from threatening to prevailing.

A Regime of Norms

Cyber deterrence alone is not a cure for all problems. Indeed, it is insufficient to ensure stability of cyberspace. This is true especially when considering how the rising distribution and automation, multiple interactions, and fast-pace performance of cyber attacks make control progressively less effective, while increasing the risks for unforeseen consequences, proportionality breaches, and escalation of responses[33]. An international regime of norms regulating state behaviour in cyberspace is necessary to complement cyber deterrence strategies and foster stability.

Over the past twenty years, the UN, the Organisation for Cyber Security and Co-operation in Europe (OSCE), and the ASEAN Regional Forum (ARF) and several national governments (G7 and G20) have convened consensus to define such a regime. The G7 Declaration is the latest of a series of successful transnational initiatives made in this direction before the failure of the UN Group of Government Experts (UN GGE) on '"Developments in the field of information and telecommunications in the context of international security"[34].

The G7 Declaration identifies two main instruments: confidence building measures (CBMs) and voluntary norms. CBMs foster trust and transparency among states. In doing so, they favour co-operations and measures to limit the risk of escalation. CBMs range from establishing contact points, shared definitions of cyber-related phenomena, and communication channels to reduce the risk of misperception, and foster multi-stakeholder approach.

Voluntary norms identify non-binding principles that shape state conduct in cyberspace. *De facto*, voluntary norms identify red lines for state-run, non-kinetic cyber attacks and, thus, fill the void created by strategic ambiguity. They stress that states

[33] G.-Z. Yang, et al., "The Grand Challenges of Science Robotics", *Science Robotics*, vol. 3, no. 14, 2018.

[34] M. Schmitt and L. Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, Just Security, 30 June 2017.

should not target critical infrastructures and critical information infrastructures of the opponent (norms 6, 8, and 11 of the G7 Declaration); should avoid using cyber attacks to violate intellectual property (norm 12 of the G7 Declaration); and remark the responsibility of state actors to disclose cyber vulnerabilities (norms 9 and 10 of the G7 Declaration).

CBMs and (in part) voluntary norms have been then included in the 2017 cyber security framework launched by the European Commission. The framework is one of the most comprehensive regulatory frameworks for state conduct in cyberspace so far. Yet it does not go far enough. The EU treats cyber defence as a case of cybersecurity, to be improved passively by making member states' information systems more resilient. It disregards active uses of cyber defence and does not include AI.

This was a missed opportunity. The EU could have begun defining red lines and proportionate responses in its latest rethink. For example, the 2016 EU directive on "Security of Network and Information Systems" provides criteria for identifying crucial national infrastructures, such as health systems or key energy and water supplies that should be protected. The same criteria could be used to define illegitimate targets of state-sponsored cyber attacks.

The EU cyber security framework remains a step in the right direction, but more work needs to be done. After the failure of the UN GGE, it is crucial that discussion on the regulation of state behaviour resume. Regional forums, such as NATO and the EU, may be a good starting point for more fruitful discussions. When considering state-run cyber defence, it is crucial that the following three steps are taken into consideration to avoid serious imminent attacks on state infrastructures, and to maintain international stability. These are:

- **Define "red lines"** distinguishing legitimate and illegitimate targets and definitions of proportionate responses for cyber defence strategies.
- **Building alliances** by mandating "sparring" exercises between allies to test AI-based defence capabilities and

the disclosure of fatal vulnerabilities of key systems and crucial infrastructures among allies.

- **Monitor and enforce rules at international level** by defining procedures to audit and oversee AI-based state cyber defence operations, alerting and remedy mechanisms to address mistakes and unintended consequences. A third-party authority with teeth, such as the UN Security Council, should rule on whether red lines, proportionality, responsible deployment or disclosure norms have been breached.

Conclusion

"Those who live by the digit may die by the digit"[35]. Indeed, if the threats coming or targeting cyberspace pose serious risks to the stability and security of our societies is because we live in societies that are increasingly more dependent on digital technologies. As Ericcson and Giacomiello put it:

> In 1962, Arnold Wolfers wrote that national security is the absence of threat to a society's core values. If modern, economically developed countries are increasingly becoming information societies, then, following Wolfers' argument, threats to information can be seen as threats to the core of these societies[36].

A relation of mutual influence exists between the way conflicts are waged and the societies waging them. As Clausewitz remarked, more than an art or a science, conflicts are a social activity. And much like other social activities, conflicts mirror the values of societies while relying on their technological and scientific developments. In turn, the principles endorsed to regulate conflicts play a crucial role in shaping societies.

---

[35] L. Floridi (2014a).

[36] J. Eriksson and G. Giacomello, "The Information Revolution, Security, and International Relations: (IR)Relevant Theory?", *International Political Science Review*, vol. 27, no. 3, 2006, pp. 221-44, p. 222.

Think about the design, deployment, and regulation of weapons of mass destruction (WMDs). During World War II, WMDs were made possible by scientific breakthroughs in nuclear physics, which was a central area of research in the years leading to the War. Yet, their deployment proved to be destructive and violent beyond what the post-war world was willing to accept. The Cold War that followed, and the nuclear treaties that ended it, defined the modes in which nuclear technologies and WMDs could be used, drawing a line between conflicts and atrocities. In doing so, treaties and regulations for the use of WMDs contributed to shape contemporary societies as societies rejecting the belligerent rhetoric of the early twentieth century and to striving for peace and stability.

The same mutual relation exists between information societies and cyber conflicts, making the regulation of the latter a crucial aspect, which does and will contribute to shape current and future societies. In the short term, regulations are needed to avoid a digital wild west, as remarked by Harold Hongju Koh, the former Legal Advisor US Department of State. In the long term, regulations are needed to ensure that cyber conflicts will not threat the development of open, pluralistic, and tolerant information societies[37].

The only way to ensure this outcome is to develop new domain-specific, conceptual, normative, and strategic framework. Analogies with kinetic conflicts, strategies to deter them, and existing normative frameworks should be abandoned altogether, as they are misleading and detrimental for any attempt to develop innovative and in-depth understanding of cyberspace, cyber conflicts, deterrence, and ensure stability. The effort is complex, but also necessary.

[37] L. Floridi and M. Taddeo, "How AI Can Be a Force for Good", *Science*, vol. 361, no. 6404, 2018b, pp. 751-52.

7. Will Authoritarian Regimes Lead in the Technological Race?

Samuele Dominioni

Many countries around the world are embracing the fourth industrial revolution[1], which is built on the dependence of layers of technologies and on the capacity to manage big data; their chances to profit and prosper from this revolution are determined by their political capacity to master it. Although tech developments are politically neutral[2], the way they are adopted, implemented and regulated is political and, in turn, technological developments have important effects on politics as well. As Susskind argued[3], in the next century, politics will be transformed by three main developments: increasingly capable systems, increasingly integrated technology and increasingly quantified society. Artificial Intelligence, with its achievements in the field of deep and machine learning, will be at the core of this revolution. The huge transformations that the fourth industrial revolution entails are affecting economies, societies and political regimes in different ways. So far, there is a common perception that authoritarian regimes are getting the better of technological developments in several fields and that liberal democracies

[1] L. Floridi, *The 4° Industrial Revolution*, Oxford, Oxford University Press, 2014.
[2] A.H. Unver, "Artificial Intelligence, Authoritarianism and the Future of Political Systems", *Cyber-Governance and Digital Democracies 09*, Center for Economic and Foreign Policy Studies, 2018.
[3] J. Susskind, *Future Politics. Living in a World Transformed by Tech*, Oxford, Oxford University Press, 2017.

are struggling with them. In February 2017, *Scientific American* featured a special issue titled: "Will democracy survive big data and artificial intelligence?"[4]. In addressing this question, the article pointed to the double-edged sword of data-driven politics, where a programmed society and programmed citizens are seen as undermining the founding principles of our constitution. This risk has also been identified by other studies that underline particular aspects of how technology is taking over liberal democracies, by altering public perception[5], for instance, and fostering polarization and echo chambers[6]. Conversely, the study published on *Scientific American* mentioned China and Singapore, which are not liberal democracies, as perfect examples of data-controlled societies[7]. Therefore, the global quest for technological leadership becomes linked with the issue of which regime type is better equipped for harvesting and managing innovations. Thus, it could be hypothesized that in the long run, authoritarian regimes, which have apparently more adaptable organizational capabilities to deal with tech developments, will be more successful in achieving positions of power in the international system.

This hypothesis relies on a compelling International Relations theory which claims that the rise and fall of global superpowers is caused by different growth rates and signs of technological

[4] D. Helbing et al., "Will democracy survive big data and artificial intelligence?", *Scientific American*, 25 February 2017.

[5] V. Polonski, "How Artificial Intelligence Silently Took Over Democracy", *World Economic Forum*, 2017; W.A.Carter, *Fear, Democracy, and the Future of Artificial Intelligence*, Center for Strategic and International Studies; Council of Europe, 2019. "AI and Democracy", Introductory speech by Snežana Samardžic-Markovic, Director General of Democracy at the High-level conference on "Governing the Game Changer – Impacts of artificial intelligence development on human rights, democracy and the rule of law", Helsinki, 26-27 February 2019.

[6] M. Del Vicario et al., "The spreading of misinformation online", in *Proceedings of the National Academy of Sciences of the United States of America*, vol. 113, pp. 554-559; F. Rugge. 2018. "'Mind Hacking': Information Warfare in the Cyber Age", ISPI Analysis, 11 January 2018.

[7] D. Helbing et al. (2017).

and organizational progress, which could favour one nation over the others[8]. According to this theory, the relative power of dominant nations is never constant and thus makes the international system unstable and complex. So far, in the contemporary world, the successful hegemonic nations, which were able to manage innovation thereby achieving a position of power, were democracies. For example, in the XIX century, Great Britain maintained a hegemonic position in the international world order, known as *Pax Britannica*, which lasted from 1815 to 1914. This *regnum* was made possible by major organizational and technological innovations in British society. In particular, with the full development of the industrial revolution, London was eventually able to expand its power overseas, establishing itself globally for almost a century. Achieving technological superiority became the *mantra* of competing powers throughout the XX century, leading to the fall of medium powers (which had to rely on the superpowers in a dependence relationship)[9] and the creation of a bipolar order. That technological race, which never resulted in open confrontation between the two superpowers, the United States and the Soviet Union, nonetheless had a winner and a loser. The "End of History" was the victorious manifestation of the *Pax Americana* and the celebration of liberal democracy as the ultimate form of government for humanity.

That, however, did not last long. In the aftermath of 9/11, and with the launch of the *war on terror*, the benign hegemony[10] built upon the pillars of multilateralism and institutionalism began to decline. Moreover, the re-emergence of Russia as a key actor since the election of Vladimir Putin and the impressive economic growth of the Chinese economy led the United States – during the Obama administration – to recognize that

[8] P. Kennedy, *The Rise and Fall of Great Powers*, Washington, Random House, 1987.
[9] B. Badie, *The Imported State: The Westernization of the Political Order*, Stanford, Stanford University Press, 2000.
[10] A. Colombo, "Trump's America and the Decline of the Liberal World", in A. Colombo and P. Magri (eds.), *The End of a World. The Decline of the Liberal Order*, Milan, Ledizioni-ISPI, 2019, pp. 31.

the distribution of power in the international system had already changed[11]. Moreover, authoritarian forms of governments began to challenge the liberal democratic paradigm once again, this time not in eschatological terms (as was the case during the Cold War) but based on claims of providing alternative and better forms of governance. This claim had a foreign policy dimension, with the rise of the so-called *revisionists* of the liberal international order[12]. We are currently living in an *interregnum*, which – quoting Gramsci – happens when "the old world is dying, and the new world struggles to be born". As such, the rise of the post-liberal or the a-polar world could be interpreted as an historical phase of re-assessment characterized by the outbreak of new and path-breaking technologies, such as Artificial Intelligence and Quantum Computing.

The changing global scenario thus entails a new set of challenges and calls for new norms that address the complex and interconnected issues of global security, including for example climate change and technological innovation[13]. As we will see in the next section, both authoritarian and democratic regimes are undergoing radical transformations, which eventually reinforce or weaken their posture in the international system. As history teaches us, one of the main drivers of maintaining or acquiring a position of power is [mastering of and innovating in] technological development. In fact, "few powerful states have been willing to restrict their pursuit of perceived technological advantages"[14]. In the current quest for technological superiority, it is easy to see what Mearsheimer affirmed about great powers' behavior "one state's gain in power is another state's loss, great powers

[11] Ibid., p. 33.

[12] See G.J. Schmitt (ed.), *Rise of the Revisionists. Russia, China and Iran*, Washington DC, AEI Press, 2018.

[13] ISPI Forum, "The Future of Multilateralism", *Senior Expert Meeting Report*, ISPI, 2019.

[14] C. Kavanagh, "New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?", Carnegie Endowment For International Peace, 2019.

tend to have a zero-sum mentality when dealing with each other. The trick, of course, is to be the winner in this competition and to dominate the other states in the system." Thus, the ongoing global quest for technological leadership between the United States and China is a 2.0 demonstration of Kennedy's theory of the "Rise and Fall of Great Powers." The race not only entails issues of hard-security but also affects the way we live and will experience technology in the coming years, and it includes mutually exclusive concepts such as liberal democracy and authoritarianism. Are democracies doomed? Will authoritarian regimes achieve a leading position in the new international order?

Regime Types and New Technologies

As stated at the outset, technology is transforming politics in three main areas: increasingly capable systems, increasingly quantified society and increasingly integrated technology. The first cluster refers to the development of technological systems such as Artificial Intelligence and Quantum computing, which allow (and will allow) extraordinary computational power. This is made possible not only by better technical processes but by much greater availability of data. In the increasingly quantified society, everyone is producing an impressive amount of data, which is used for economic and political purposes. By 2025, worldwide data is expected to grow to at least 175 zettabytes[15]. The technological dependency of many societies is determined, to a certain extent, by its increasing integration. For example, with the development of the Internet of Things the digital is everywhere, it is pervasive and inseparable from our daily experience. As briefly mentioned in the introduction, even though technology is politically neutral, the way it is implemented is deeply political.

[15] D. Reinsel, J. Gantz, and J. Rydning, "The Digitization of the World From Edge to Core", IDC White Paper, November 2018.

In authoritarian countries, the near-term impact of technology adoption and implementation is more ominous[16]. The example of Singapore as a perfect data controlled society is emblematic of their original capacity to adapt to technological innovation. Surprisingly, for many years, the development of telecommunication (TLC) systems around the world has been portrayed as a possible cause of crisis for the stability of authoritarian regimes. Indeed, it was thought that the latter were not able to withstand the free sharing of information which TLC implied. Accordingly, those who supported the theories of globalization claimed that thanks to rapid technological advances in TLC and transportation, we would witness increased flows of cultural values across nations. This "cosmopolitan communication"[17] would foster the spread of democratic values such as tolerance and freedom, which would result in a growing number of cosmopolitan societies. The Arab Spring case has often been portrayed as a perfect example of this effect[18]. However, in less than a decade this picture has been turned upside-down: in many countries, the technologies that many heralded as tools of liberation are now used effectively to repress dissent and curb civil and political rights[19]. These events were a wake-up call for authoritarian regimes, which are proving to be extremely adaptive to new technologies.

According to Deibert[20], authoritarian regimes operate at three different levels in the way they tackle technological development. Those using *First-generation controls* are more interested in blocking and isolating their polity from information

---

[16] B. Scott, S. Heumann, and P. Lorenz, *Artificial Intelligence and Foreign Policy*, January 2018, pp. 28.

[17] P. Norris, *Why election fail?*, Cambridge, Cambridge University Press, 2015.

[18] W. Ghonim, *REVOLUTION 2.0 The Power of the People Is Greater Than the People in Power: A Memoir*, Houghton Mifflin Harcourt, 2012; H.H. Khondker, "Role of the New Media in the Arab Spring", *Globalization*, vol. 8, no. 5, 2011.

[19] R. Deibert, "Cyberspace under siege", in Larry Diamond et al. (eds.), *Authoritarianism goes Global. The Challenges to Democracy*, Baltimore, John Hopkins University Press, 2016.

[20] Ibid.

spreading. One of the most notorious and successful examples of this is the Great Firewall of China[21], but many other countries have adopted different types of First-generation controls (including Iran, Pakistan, Saudi Arabia, Bahrain, Yemen, and Vietnam). Then there are *Second-generation controls*, aimed at deepening and extending information controls in society through laws, regulations and various forms of "baked-in" functionalities that governments require manufacturers and service providers to build into their products. For example, the "AI transformation in data processing – including facial and voice recognition at scale, code-breaking, and fact-pattern correlation – is a game-changer for intelligence and law-enforcement surveillance operations"[22]. "With its interest in surveillance and censorship driven by concerns for national security," such as the "social credit system", "China has emerged as a leader in AI-enabled surveillance"[23]. Finally, *Third generation controls* refer to those authoritarian regimes that are on the offensive in the cyber arena. Malicious cyber campaigns aimed at interfering with democratic electoral processes around the world, punitive actions conducted through cyber-mercenaries against selected targets or cyber attacks against bank accounts aimed at stealing money are just some examples of offensive actions conducted in the fifth domain by some authoritarian regimes. In this regard, Russia, "Iran, North Korea and China are consistently indicated in Western intelligence assessments and official statements as the main actors of direct or state-sponsored offensive campaigns in or through cyberspace"[24]. In the light of the ongoing technological race and militarization of cyberspace, this could create new instability as the capacity to project power in cyberspace

[21] For example, see D. Cheng. "China and Cyber: The Growing Role of Information in Chinese Thinking", in F. Rugge (ed.) (2018).

[22] B. Scott, S. Heumann, and P, Lorenz (2018); S. Zuboff, *The Age of Surveillance Capitalism*, New York, Public Affairs, 2018.

[23] B. Scott, S. Heumann, and P, Lorenz (2018)

[24] F. Rugge, "An 'Axis' Reloaded?", in Idem (ed.), *Confronting an "Axis of Cyber"? China, Iran, North Korea, Russia in Cyberspace*, Milan, Ledizioni-ISPI, 2018, pp. 16.

is becoming one of the assets of power politics projection as a whole. As Lewis claims "[c]yberspace has become the primary battleground for conflict between sovereignty and universal values, and between democracies and authoritarians"[25]. For example, according to Polyakova and Meserole, "Russia and China have developed and exported distinct technology-driven playbooks for authoritarian rule"[26]; these playbooks aim to strengthen nondemocratic regimes and counter Western efforts to promote democracy. Therefore, since the inception of *Third generation controls* and the global quest for technological supremacy, the ongoing competition in the digital domain concerns not only conflicting interests but also the opposition between different systems and mutually antagonistic regimes.

Thus far, with regards to the political implications of the adoption of innovative technology in liberal democracies, most of the literature has pointed to the inner perils of the widespread and uncontrolled adoption of technology into this regime type[27]. The previously mentioned article "Will democracy survive big data and artificial intelligence?" asked if Big Brother is becoming a reality and whether the essence of the democratic regime type is therefore already faltering. Indeed, many liberal democracies are already in the middle of the political transformation brought about by increasingly capable systems, increasingly integrated technology and increasingly quantified society. The risk that "the more is known about us, the less likely our choices are to be free and not predetermined by others"[28] is one

[25] J. Lewis, "Defining rule of behaviors for Force and Cooperation in Cyberspace", in ibid.

[26] A. Polyakova and C. Meserole, *Exporting digital authoritarianism: The Russian and Chinese models*, Policy Brief, Brookings, 2019.

[27] See for example: V. Polonski, "How Artificial Intelligence Silently Took over Democracy", World Economic Forum, 9 August 2017; V. Motupalli, "How Big Data is Changing Democracy", *Journal of International Affairs*, Columbia University, SIPA, 22 June 2018. M. Del Vicario et al., "The spreading of misinformation online", PNAS, vol. 113, no. 3, 19 January 2016.

[28] Dirk Helbing et al. 2017. "Will democracy survive big data and artificial intelligence?". Scientific American, 25 February.

of the possible outcomes of technology adoption in liberal democracies, as already experienced during a number of elections. The US presidential vote in 2016 highlighted the relevance of new challenges to the democratic electoral process, such as fake news and digital disinformation, nudging, hate speech and social platform censorship, echo chambers and social engineering. As the Council of Europe recently stated in its declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes published in February 2019, "these effects […] may lead to the corrosion of the very foundation of the Council of Europe. Its central pillars of human rights, democracy, and rule of law are grounded on the fundamental belief in the equality and dignity of all humans as independent moral agents"[29]. Therefore, the call for an ethical regulation of technology adoption in liberal democracies is mounting among scholars and institutions in order to safeguard the core principles of our liberal order[30].

However, the process of policy formulation, adoption, and implementation in liberal democratic regimes is longer compared to authoritarian regimes and, unlike them, it has to abide by two key procedural dimensions: the rule of law and accountability[31]. In any case, the transformations that technological developments bring into democratic polities should not be seen exclusively with concerns and from negative standpoints. Indeed, digital innovation – in particular AI – may enhance the quality of some of the values related to the principles of

[29] Council of Europe, 2019, "AI and Democracy" - Introductory speech by Snežana Samardžic- Markovic, Director General of Democracy at the High-level conference on "Governing the Game Changer – Impacts of artificial intelligence development on human rights, democracy and the rule of law", Helsinki, 26-27 February 2019, https://www.coe.int/en/web/data-protection/-/declaration-by-the-committee-of-ministers-on-the-manipulative-capabilities-of-algorithmic-processes

[30] M. Kumm (2013), "The Cosmopolitan turn in constitutionalism: an integrated conception of public law, 20 Indiana J Global Legal Studies 605", quoted in P. Nemitz, "Constitutional democracy and technology in the age of artificial intelligence". *Philosophical Transactions Royal Society A.* 376, 9, 2018.

[31] L. Morlino, "What is a 'good' democracy?", *Democratization*, vol. 11, no. 5, 2007.

democracy. For example, thanks to AI a government could be more responsive when it has to devise solutions to complex and unexpected problems. Or it could help enhance the transparency of public administration. For example, in 2016, a civil society group of tech-volunteers in Brazil launched Operation Serenata de Amor, an Artificial Intelligence project for analysing public expenditures, which became very successful and popular. In this regard, nowadays liberal democracies are confronted with new demands for direct forms of participation, which could contribute to "improving the quality of democracy and facilitating a not intermittent citizens' participation" [32] and at the same time enhance the legitimacy of representative institutions[33]. Therefore, technology is at the core of two main challenges to liberal democratic regimes. On one side, they are competing with other regime types over technology adoption and capabilities while, on the other, they have to cope with the increasing demand for new forms of participation from their polities. This is a crucial crossroads for liberal democracies.

The picture sketched above is quite negative. So far, some authoritarian regimes have exploited the three main transformative dimensions (increasingly capable systems, increasingly integrated technology and increasingly quantified society) to strengthen their postures within and outside their polity. At the same time, liberal democracies are struggling to find a proper way to adopt technological innovations into their polities while preserving and guaranteeing their founding principles. The implications of the global quest for technological supremacy between the United States and China, thus, have profound implications for the sustainability and the endurance of different political regimes. In the next session, I am going to show why authoritarian regimes are eventually unlikely to be the winners in the ongoing race.

---

[32] M. Sorice, *Between Direct Representation and Participatory Democracy*, in S. Dominioni, *Elections and Cyberspace: The Challenge of Our Democracies*, ISPI Dossier, 23 May 2019.

[33] Ibid.

The Inner Limits of Authoritarian Regimes

In the current race, authoritarian regimes seem to be better equipped. However, in this chapter, I argue that their innovation path is scarcely sustainable and that they will eventually fail to attain the leadership, unless they transition to liberal democratic rule. This claim finds its *raisons d'être* in the extensive literature that analyses the relationship between socio-economic conditions and political institutions. The idea is that the link between economic development and democracy is "one of the strongest correlations we find in the social sciences"[34]. In turn, other studies point to the fact that authoritarian regimes have more variance in their economic performances and that their economic development tends to be driven by labour exploitation[35]. More recently, Acemoglu and Robinson have argued in a seminal book[36], that the success or failure of nations is determined by the type of institutions (both economic and political) they have. In particular, the authors conceptualize institutions according to the dichotomy of extractive and inclusive. In political terms, inclusive institutions are those that are sufficiently centralized and pluralistic; in turn, extractive institutions are where one or both of these characteristics are lacking and where power is concentrated in the hands of small elites that can exercise it without many constraints. From an economic perspective, inclusive institutions are those that allow and encourage participation by the mass of the population in economic activities that make the best use of their talents and skills. As such, the authors point to the fact that "inclusive economic

[34] J.A. Cheibub and J.R. Vreeland, "Economic Development and Democratization", in N.J. Brown (ed.), *The Dynamics of Democratization. Dictatorship, Development, and Diffusion*, Baltimore, The John Hopkins University Press, 2011, p. 145.

[35] A. Przeworski, M. Alvarez, J.A. Cheibub, and F. Limongi, *Democracy and Development: Political Institutions and Well-Being in the World., 1950-1990*, Cambridge, Cambridge University Press, 2000.

[36] D.Acemoglu and J.A. Robinson, *Why Nations Fail*, New York, Crown Business, 2012.

institutions pave the way for two other engines of prosperity: technology and education"[37]. These institutions also guarantee and secure private property, rule of law, and level playing field services for all economic actors. By contrast, extractive economic institutions are those where uncertainty about rules and disincentives to entrepreneurship prevail. It goes without saying that extractive institutions are mostly found in authoritarian regimes whereas inclusive institutions are found in democratic regimes. As a matter of fact, "inclusive economic institutions will neither support or be supported by extractive political ones"[38] but actually foster a virtuous circle logic with inclusive political institutions that can persist over time.

Nevertheless, there are some cases, in which extractive political institutions are supportive of some forms of inclusive economic institutions. China is one of the most important cases in point. Over the last decade, China has shown huge signs of progress in innovation, making it one of the most interesting case studies regarding the combination of extractive and inclusive institutions. There is broad agreement nowadays that China is catching up to the United States in innovation and technology capabilities[39]. The key determinant for the linkage between exclusive political institutions and some form of inclusive economic institutions is the strong centralization of political power exercised by the Chinese Communist Party, which has sufficient *dirigiste* strength to channel resources toward the high productivity areas. The launch of the directive "Made in China 2025" in 2015 was aimed at upgrading the country's economic structure and growth model by boosting innovation, promoting the structural transformation of industries and firms and investing in human capital and talent development[40]. However,

---

[37] Ibid., p. 77.

[38] Ibid., p. 82.

[39] R.D. Atkinson and C. Foote, "Is China Catching Up to the United States in Innovation?"*, Information Technology & Innovation Foundation*, April 2019.

[40] Shang-Jin Wei. "Why Made in China 2025 should scare Donald Trump less than those betting on Chinese tech dominance", *South China Morning Post,* 27

according to several economists[41], this goal will not be sustainable unless it is followed by major governance reforms, as a way to spark a virtuous and self-reinforcing circle of inclusive economic and political institutions.

As shown by Amighini, China – despite the impressive growth rate displayed during the last decade and its increasing national innovation capacities – "still performs rather badly by some international standards [including] the quality of science."[42] Moreover, according to OECD data, Chinese efforts in research and development (R&D) are "more oriented towards experimental development rather than research, which leads to higher patentable knowledge"[43]. Hence, Amighini continues, "[i] nnovation results mainly from collocating and agglomerating externalities, which facilitate the absorption of innovation from other regions[44] rather than from R&D investments, human capital endowments and knowledge spillovers"[45]. As a matter of

June 2018.

[41] See for example: H. Wagner, "On the (Non-)sustainability of China's Development Strategies", *The Chinese Economy*, vol. 52, no. 1, 2019, pp. 1-23; A. Amighini (ed.), *China's Race to Global Technological Leadership*, Milan, Ledizioni-ISPI, 2019; D. Acemoglu and J.A. Robinson (2012).

[42] A. Amighini, "Beijing: Ready for Global Technology Leadership?", in A. Amighini (2019).

[43] Ibid., p. 28. This is demonstrated for example by the huge rise in the so-called "unicorns" (start-ups worth more than $1 billion) mostly in the e-commerce sector. According to some, these unicorns in China are flourishing because they are following the government line instead of business sense, which is detrimental for innovation. See https://www.scmp.com/business/companies/article/2139684/heart-chinas-techno-nationalism-hit-list-200-unicorns

[44] Due to the "Made in China 2025" program each region is assigned to focus on a particular aspect of technological development. See M.J. Zenglein and A. Holzmann, "Evolving Made in China 2025. China's industrial policy in the quest for tech leadership", *Merics Papers on China*, no. 8, July 2019.

[45] A. Amighini (ed.) (2019), pp. 31; J. Gerring, P. Bond, W.T. Barndt, and C. More, "Democracy and Economic Growth a Historical Perspective", *World Politics*, vol. 57, 2005, pp. 323-354; H. Landemore, *Democratic Reason: Politics, Collective Intelligence, and the Rule of the Many*, Princeton, Princeton University Press, 2012; A. Schedler, *The Politics of Uncertainty: Sustaining and Subverting Electoral Authoritarianism*, Oxford, Oxford University Press, 2013; R.D. Atkinson and

fact, China suffers from a lack of social capital as "most Chinese firms operate with hierarchical forms of organization, and there is little room for creative contributions from employees"[46], and free entrepreneurship is hampered by extractive political institutions. Moreover, as revealed by a survey conducted by the Ministry of Industry and Information Technology, the top 30 Chinese tech conglomerates "depend on foreign suppliers for 95 per cent of the advanced manufacturing and testing components on production lines for various sectors"[47]. As reported by the state-run Xinhua news agency, Chinese President Xi Jinping said that China must grasp core technologies "with our own hands", as they are key to national security and high-quality economic development[48]. Xi's sentence is emblematic of the structural challenges facing China's national innovation system. In fact, Chinese economic institutions are still far from being fully inclusive, and this could prevent China from taking the lead in the innovation sector. Indeed, in order to catch up and be ahead in the innovation sector, a country cannot simply transfer and copy technologies from other countries, nor it is sufficient for it to boost and improve *dirigiste* programs domestically. It requires firms that have "accumulated indigenous technological capability to generate emerging technologies in the fluid stage and challenge firms in [other] countries"[49]. This goal can only be achieved through a shift in the role of political

C. Foote (2019); Luciano Floridi, *The 4° Industrial Revolution*, Oxford, Oxford University Press, 2014.

[46] B.-Å. Lundvall, *The Learning Economy and the Economics of Hope, Anthem Studies in Innovation and Development*, Anthem Press, 2016 pp. 281-282, quoted in: A. Amighini (2019).

[47] He Huifeng, "Beijing did a tech reality check on its industrial champions. The results were not amazing", *South China Morning Post*, 18 July 2018.

[48] Ibid.

[49] K. Linsu, *Imitation to innovation: The Dynamics of Korea's Technological Learning*. Boston, Harvard Business School Press, 1997, quoted in R.D. Atkinson and C. Foote, "Is China Catching Up to the United States in Innovation?", *Information Technology & Innovation Foundation*, April 2019, pp. 2.

institutions "from director to enabler"[50], a role that extractive political institutions are unlikely to be able play. Therefore, in order to play a (sustainable) leading role in the quest for technological superiority, China should address challenges and inefficiencies related to institutions and governance as well as to organizational capacity and social barriers.

This section has given a brief description of the inner limits of the Chinese innovative framework. Although there are other examples of authoritarian regimes combining economic growth with *Third generation control* of digital technologies, they are not included in this short analysis as they are still at the margins of the global quest for technological superiority. In the case of Singapore, for example, while it is portrayed as the most successful model of digital authoritarianism, its intrinsic characteristics (such as being a small state) will prevent it from being one of the competitors when it comes to hegemonic power. Moreover, Acemoglu and Robinson's theory of inclusive/extractive political/economic institutions can be applied to many other countries, even to the so-called hybrid regime, which "displays lower levels of business confidence, […] and more frequent formal institutional disruption than either democracies or autocracies"[51]. Wherever there are extractive institutions, economic growth – and thus innovation – is hardly sustainable. We are not claiming that economic growth is impossible under authoritarian rule, but that at some point extractive growth will reach limits, which will require inclusive reforms to overcome.

Concluding reflections

It goes without saying that the same types of constraints are not found in democratic regimes. Here inclusive economic and

[50] R.D. Atkinson and C. Foote (2019).

[51] H.E. Hale, "Hybrid Regimes. When Democracy and Autocracy Mix", in H.E. Hale (ed.), *The Dynamics of Democratization. Dictatorship, Development, and Diffusion*, Baltimore, The John Hopkins University Press, 2011, pp. 40.

political institutions foster the so-called virtuous circle. The latter "arises not only from the inherent logic of pluralism and the rule of law but also because inclusive political institutions tend to support economic institutions"[52]. This is particularly true, as demonstrated in a ground-breaking article[53], when democracy in a country is considered in terms of its accumulated stock of democracy rather than its level of democracy at a particular moment in time. Therefore, the longer a country has been a democracy over time the more it fosters sustainable economic growth and innovation through four types of capital: *physical, human, social and political*. These form the foundation of what is called the *epistemic superiority* of democracy[54], which claims that, because of its inclusive institutions, political actors in democratic settings can make smarter decisions than those in authoritarian ones, which suffer from informational uncertainty[55]. However, although China will not be changing its political regime in the short-medium term, and thus will hardly be in position to take the lead, it "can make an enormous progress, including in science and engineering industries. And that progress will significantly harm global innovation leaders (firms and nations)"[56]. Therefore, it is crucial that liberal democracies should not lower their guard: the success of liberal democracies will also depend on their ability to cope with the inner challenges posed by technology to their polities and to their capacity to keep boosting innovation while preserving the integrity of their founding principles.

---

[52] D. Acemoglu and J.A. Robinson (2012), p. 309.

[53] J. Gerring, P. Bond, W.T. Barndt, and C. More, "Democracy and Economic Growth a Historical Perspective", *World Politics*, vol. 57, 2005, pp. 323-354.

[54] H. Landemore, *Democratic Reason: Politics, Collective Intelligence, and the Rule of the Many*, Princeton, Princeton University Press, 2012.

[55] A. Schedler, *The Politics of Uncertainty: Sustaining and Subverting Electoral Authoritarianism*, Oxford, Oxford University Press, 2013.

[56] R.D. Atkinson and C. Foote (2019).

Therefore, the United States (US) and European Union (EU) should keep investing in the so-called foundational technologies (e.g. semiconductors) but also on core technologies such as artificial intelligence and quantum computing, which are the enabler for future applications both in the civil and military spheres. Moreover, as is already happening in both the US and EU, fostering the concept of "security by design" will be decisive for the reliability of our TLC. For example, it will be key to reduce dependence on critical components from China, or to make certification mandatory on tech components imported from abroad (such as those envisaged in the EU Cybersecurity Act). Finally, Western countries (and other like-minded states) would be well advised to keep working at the international level to push forward shared norms and ethical standards on the adoption of new technologies with a focus on preserving privacy and human rights. Overall, it can be argued that due to existing differences in long term growth rate performances as well as differences in innovation and organizational capacity between democratic and authoritarian regimes, the latter are unlikely to succeed in taking the lead in the global quest for technological supremacy and, thus, the balance of power in the international system will not change.

The Authors

John R. Allen currently serves as the 8th president of the Brookings Institution. He is a retired US Marine Corps four-star general and former commander of the NATO International Security Assistance Force and US Forces in Afghanistan. Prior to his role at Brookings, Allen served as senior advisor to the secretary of defense on Middle East Security and as special presidential envoy to the Global Coalition to Counter ISIL. Allen is the first Marine to command a theater of war, as well as the first Marine to be named commandant of midshipmen for the US Naval Academy. Beyond his operational and diplomatic credentials, Allen has led professional military educational programs, including as director of the Marine Infantry Officer Program and commanding officer of the Marine Corps Basic School. Allen was the Marine Corps fellow to the Center for Strategic and International Studies and the first Marine officer to serve as a term member of the Council on Foreign Relations, where today he is a permanent member. Among his other affiliations, Allen is a senior fellow at the Merrill Center of the Johns Hopkins School of Advanced International Studies and a senior fellow at the Johns Hopkins Applied Physics Laboratory. He is an "Ancien" of the NATO Defense College in Rome, and a frequent lecturer there. Allen is also the recipient of numerous US and foreign awards.

Samuele Dominioni is a research fellow at the ISPI Centre on Cybersecurity, in partnership with Leonardo. Before joining ISPI he was post-doctoral researcher at the Forum Internationale Wissenschaft (University of Bonn). He also worked as consultant and researcher for European Union funded projects, for the Venice Commission (Council of Europe), and the Office of Democracy and Human Right at the Organisation for Security and Cooperation in Europe (OSCE/ODIHR). He was lecturer at the Institut d'Etudes Politiques de Paris (Sciences Po), and visiting scholar at the Department of Political Sciences at Columbia University (New York) and at Ivane Javakhishvili University in Tbilisi (Georgia). He published several contributions in high-level academic outlets and provided policy reports for the European Commission and the Council of Europe.

Giampiero Massolo is the president of ISPI. Early in his diplomatic career, he served in Moscow and Brussels. He has served in several high-ranking positions in the Italian government, such as deputy diplomatic advisor to the Prime Minister and deputy secretary-general of the Ministry of Foreign Affairs. In January 2006, he was appointed to the rank of ambassador and in 2007 he became secretary-general of the Ministry of Foreign Affairs, the highest position in the Italian diplomatic career. He has served as the personal representative of the Italian prime minister for various G8 and G20 Summits. Finally, from 2012 to 2016 he was the director general of the Department for Intelligence and Security, the coordinating body of the Italian intelligence community. Ambassador Massolo is also a member of the executive committee of Aspen Institute Italia.

Gabriele Rizzo, Ph.D., APF, is a visionary futurist and an enthusiastic innovator. He is principal futurist and trusted advisor for United States and NATO, member at Large for Strategic Foresight in NATO STO and chairman of the Future Technology track in NATO ACT Futures Work – an oeuvre framing deep futures out to 2040-2060, to inform $1T worth

of Defense planning. Rizzo also serves as professor of strategy at La Sapienza University; visiting professor at NATO Defense College, and as an advisor to the Italian Joint Staff. He is one of the few NATO Early Career Nuclear Strategists and one of the just 15 Alliance's Young Disruptors. He held multiple positions over more than ten years in engineering staff before moving to strategy, where he contributed substantially to strategic visions and long-term thinking of United States, Italy, Switzerland, European Defense Agency, NATO, Fortune Global500 industries, and international organisations with billion-sized budget. He has more than 40 publications to his credit, authored several capstone works on deep futures and was honored with national and international awards.

Counselor **Fabio Rugge** is head of ISPI's Centre on Cybersecurity, in partnership with Leonardo. He is a diplomat currently working as head of the Office in charge for NATO and Security and Politico-Military Issues, Directorate General for Political Affairs and Security, Ministry of Foreign Affairs and International Cooperation. From 2012 to 2016 he worked at the Italian prime minister's Office and prior to that he was counselor at the Italian Delegation to the North Atlantic Council in Brussels and Consul General of Italy in Mumbai (India). He held several positions at the Ministry of Foreign Affairs and International Cooperation in Rome – among others at the Policy Planning Unit and as head of the Office in charge for scholarships and the internationalisation of Italian Universities. Rugge is adjunct professor of Cyber Diplomacy at LUMSA University. He held courses and lectures in several Italian universities on Cybersecurity and International Relations.

Rear Admiral **David Simpson**, USN (Ret.), is a professor at Virginia Tech's Pamplin College of Business. He served as chief of the US Federal Communication Commission's Public Safety and Homeland Security Bureau from 2013 to 2017. As bureau

chief, he oversaw public safety, homeland security, emergency management, cybersecurity, and disaster preparedness activities at the FCC, and worked with public and private partners to deliver state-of-the-art communications that were accessible, reliable, resilient, and secure. He previously served as vice director of the Defense Information Systems Agency (DISA) and as Director for Communications and Information Services for US Forces Iraq.

Tom Stefanick is a visiting fellow in Foreign Policy at the Brookings Institution. He is writing a book on the impacts of AI on the military to be published by Brookings Press in 2020. From 1988 to 2018 he was a technical analyst and eventually a senior vice president at Metron, Inc., consulting mainly to the Navy. He led R&D efforts in machine learning, image recognition, lidar, autonomous planning, statistical modeling, sensor modeling, and computer simulation of naval operations. Prior to joining Metron in 1988, he was a science fellow in HASC working on Soviet submarine and strategic antisubmarine technology. He is the author of *Strategic Antisubmarine Warfare and Naval Strategy* (1987).

Mariarosaria Taddeo is research fellow at the Oxford Internet Institute, University of Oxford, where she is the deputy director of the Digital Ethics Lab, and is faculty fellow at the Alan Turing Institute. Her recent work focuses mainly on the ethical analysis of Artificial Intelligence, cyber security , cyber conflicts, and ethics of digital innovation. Her area of expertise is Philosophy and Ethics of Information, although she has worked on issues concerning Epistemology, Logic, and Philosophy of AI. She has been listed among the top 50 most inspiring Italian women working in AI in 2018. In the same year ORBIT listed her among the top 100 women expert in AI on a global scale. Taddeo has been awarded The Simon Award for Outstanding Research in Computing and Philosophy. She also received the World Technology Award for Ethics

acknowledging the originality and her research on the ethics of cyber conflicts, and the social impact of the work that she developed in this area. Since 2016, she serves as editor-in-chief of *Minds & Machines* (SpringerNature) and of *Philosophical Studies Series* (SpringerNature).

John Villasenor is a nonresident senior fellow in Governance Studies and the Center for Technology Innovation at Brookings. He is also a professor of electrical engineering, law, and management at UCLA, as well as a member of the Council on Foreign Relations. Villasenor's work considers the technology, policy, and legal issues arising from key technology trends including the growth of artificial intelligence, the increasing complexity and interdependence of today's networks and systems, and continued advances in computing and communications. He has written for the *Atlantic*, *Billboard*, *the Chronicle of Higher Education*, *Fast Company*, *Forbes*, *Los Angeles Times*, *New York Times*, *Scientific American*, *Slate*, and *the Washington Post*, and for many academic journals. Prior to joining the faculty at UCLA, Villasenor was with the NASA Jet Propulsion Laboratory, where he developed methods of imaging the earth from space.

Tom Wheeler is a professor at Virginia Tech's Pamplin College of Business.He was the 31st *chair* of the FCC from 2013 to 2017. Currently, he is a visiting fellow at the Brookings Institution.