Ilmin International Relations Institute

No. 54

IIRI Online Series

Back to the Future?

The Fourth Industrial Revolution's Impact on International Relations

다니엘 코놀리

고려대 국제대학원 연구교수

2019. 11. 25

일민국제관계연구원
Ilmin International Relations Institute

Back to the Future? The Fourth Industrial Revolution's Impact on International Relations

다니엘 코놀리(Daniel Connolly)|
고려대 국제대학원 연구교수

Introduction

The Fourth Industrial Revolution (4IR) is a popular buzzword used by economists, entrepreneurs, educators and policymakers to describe a series of looming technological changes expected to drastically alter the global economy. Although greeted with great optimism by many, these changes also raise the specter of massive job losses and social disruption due to widespread automation. As a result, governments around the world are moving to embrace the opportunities of the 4IR while mitigating its risks. Korea was one of the early movers, launching its Presidential Committee on the Fourth Industrial Revolution (PCFIR) in October 2017.

But what does the 4IR mean for international relations? Current discussions are largely centered on domestic economic and societal impacts. In this vein, PCFIR's mandate focuses on devising policies to facilitate "Korean society's adaptation" to 4IR technologies.[1] Although such domestic issues are important to consider, it is also necessary to explore the 4IR's potential impacts on the international system. This paper begins by putting forward a comprehensive definition of the 4IR that highlights its linkage with earlier concepts in the field of security studies, especially the Revolution in Military Affairs (RMA). This linkage allows us to filter out some of the hype in current 4IR discussions and focuses our attention on real-world processes that are shaping international relations, namely the securitization of dataflows, distributed warfare, and the political economy of new technologies.

What is the 4IR?

Many popular definitions of the 4IR narrowly focus on its core technologies, such as blockchain, artificial intelligence, 5G, and nanotechnology; or its anticipated consequences, such as automation or the blurring together of digital, physical and biological spaces. However, a comprehensive definition of the 4IR, derived from engineering and managerial literature, understands it as a conceptual shift in how organizations and individuals approach data and decision-making. This new approach seeks the creation of cyclical processes of datafication (translating real-world objects into digital traces), distribution (sharing the digital traces within or between organizations), and decision-making (when the digital traces are used to act upon the real-world). In short, the 4IR consists of businesses eagerly using new technologies to digitalize all aspects of their operations and accelerate the flow of real-time data to decision-makers, who may not even be human.[2]

Does this sound familiar? It should. In fact, international relations scholars were talking about the 4IR decades before it became a

[1] "Presidential Committee on the Fourth Industrial Revolution," accessed November 18, 2019, https://www.4th-ir.go.kr/home/en.

[2] A common example of this in the engineering literature are smart machines that order their own replacement parts or schedule their own maintenance.

buzzword. We knew it back then as the Revolution in Military Affairs (RMA). This concept, drawing upon an even earlier Soviet theorization of Reconnaissance-Strike Complexes, anticipated that the use of precision weapons, networked sensors and shooters, and the sharing of real-time information would revolutionize warfare by allowing more accurate and quicker decision-making. In fact, the language used by these documents was almost identical to contemporary discussions of the 4IR except they speak about delivering fire support rather than personalized products for customers. For this reason, the discrediting of RMA concepts during long insurgencies in Iraq and Afghanistan suggests that IR scholars can contribute to current 4IR discussions by critically exploring why early optimistic predictions of digital transformation in the military sphere never came true. Likely factors include cost, resistance by key stakeholders, technical complexity, and unexpected challenges arising from abundance, meaning that more data does not make decision-making easier or better. These lessons, which can be found in past IR scholarship, are especially relevant today because enterprises and governments around the world are embarking on similarly expensive and potentially flawed plans for digital transformation.

Key Impacts

Although the hype surrounding the RMA faded away by the 2010s, many of its underlying technologies, concepts, and practices survived and proliferated horizontally across the international system as well as downward into national governments, societies, and economies. Indeed, this process of proliferation led to early concepts like Industry 4.0, which focused on smart factories, and then the 4IR, which envisions smart societies. Ironically, the hype surrounding the domestication of these technologies, and their re-appearance as consumer items such as self-driving cars, has distracted attention away from their growing impacts on the international system, which have been gestating for decades.

The first issue is the securitization of dataflows. The informatization of warfare in the late 1980s and 1990s, which the Soviet Union could not afford, contributed to the collapse of the bipolar system and the establishment of US hegemony. The US-led world order benefited from global systems of datafication and distribution, perhaps best exemplified by the GPS satellite system (a key enabler of precision weapons) and the Internet. In this period, US policymakers were optimistic about the power of global information flows. For example, the US Navy Research Lab (NRL) even funded research on onion routing, which allowed truly anonymous access to the Internet. This period also coincided with highly laudatory accounts of the RMA that portrayed it as something uniquely American. In short, informatization was considered synonymous with democratization at the unit-level and the creation of an international system friendly to US interests at the system-level.

The terrorist attacks on 9/11 shattered this confidence. Al-Qaida used commercial PC flying simulators and the internet to coordinate the most devastating attack in US history.[3] In fact, the War on Terror has witnessed non-state actors using modern technologies in inventive ways, a process that Israeli security expert Itai Brun calls the “Other RMA.”[4] This has included Iraqi insurgents hijacking the camera feeds of US drones, consumer electronics being used as weapon delivery systems, and Islamic State’s widespread hijacking of social media networks. Even the Tor browser has been used to coordinate the operations of terrorist cells while state adversaries such as Russia and North Korea have launched successful fake news operations and cyberattacks on US companies and

[3] The use of simulations, also known as Digital Twins in the engineering literature, is an important part of the 4IR data cycle because they allow systems to be iteratively tested and modified in the virtual world.

[4] Itai Brun, “‘While You’re Busy Making Other Plans’ – The ‘Other RMA,’” *Journal of Strategic Studies* 33, no. 4 (August 2010): 535–65, https://doi.org/10.1080/01402390.2010.489708.

citizens. Real-time dataflows and universal connectivity, once seen as the West's unique source of strength, are now seen as vectors of risk, as exemplified by recent debates among US policymakers about the "safety" of telecommunications equipment from Huawei and fears that Chinese-made consumer drones sold via Amazon are spying on their users.

Second, the proliferation of 4IR technologies are facilitating new forms of distributed and automated warfare that directly challenge the primacy of the US and its regional allies. Although the US military pioneered the use of many of these smart systems and techniques, such as remote warfare, in retrospect this was only a temporary head-start. Non-state groups such as Hezbollah and Hamas, are increasingly attaining rudimentary precision-targeting capabilities while rival states such as China, Iran and even North Korea are investing in varieties of anti-access and area denial systems (A2/AD) designed to erode US force projection capabilities. For the foreseeable future, US weapons will continue to be smarter, but the proliferation of smart weapons and delivery systems is changing the face of war. If we remember that early theorists of the RMA intended to use precision weapons to attain nuclear-like levels of destruction without the inconvenience of radioactive fallout, the risk surrounding the proliferation of these weapons takes on a new urgency. Especially, these systems allow actors to engage in risky and escalatory behavior, such as covert strikes, which blur the boundaries between peace and war. This threat was demonstrated by the drone and missile attacks on the Saudi Aramco oil refinery complexes in September 2019, which reduced the country's oil production significantly. With the identities of the attackers shrouded in ambiguity, regional actors were unable to muster a coordinated response.

Finally, attempts to respond to these insecurities are complicated by the political economy of new technologies. Unlike nuclear weapons, which confer strategic power but may entail considerable economic tradeoffs, the technologies of the 4IR are dual-use resources that simultaneously improve a state’s military and economic power. For example, the same pattern recognition algorithms that help a delivery drone navigate a busy city will also help guided missiles find a US aircraft carrier in the vastness of the Western Pacific. Indeed, some emerging technologies, like artificial intelligence and quantum computing, will have profound strategic consequences because they enable vastly accelerated processing, transmission and use of data by governments, private corporations and militaries alike. Although US and Chinese economic interdependence helped create a stable Pacific in the era of globalization, it is uncertain that this relationship can continue in the digital age because competitive logics in the military and commercial fields are converging. Even China’s peaceful rise as an AI power will give it instant military advantages, a future that the US cannot accept.

Conclusion

Real-time data cycles have immense economic potential and military potency. The 4IR is often seen as something new and historically unique, but it has roots in the RMA, an innovative Post-Cold War doctrine embracing digitalization, multidirectional information distribution, and real-time decision-making. But these systems are incredibly complex and fragile. On one hand, IR scholars can contribute to over-hyped discussions of new technologies by examining the practical and political challenges that states and militaries faced in implementing the RMA in the 1990s and early 2000s. These challenges will likely reoccur in the context of the 4IR. On the other hand, IR scholars have a pressing need to better understand the subsequent proliferation of RMA-like concepts and technologies, especially their diffusion into the civilian sphere. These systems, once celebrated for cementing US unipolarity, are now creating a more complex, dynamic, and dangerous international system by enabling new forms of insecurity, which are conceptualized here as dangerous or hijacked dataflows and distributed warfare. But perhaps the most serious risk is that 4IR innovation is raising the stakes of great power economic and military competition. Rather than today’s interpenetrated global technologies, like the Internet, the 4IR may become an era of divergence. China’s Great Firewall and Iran’s Halal Net are not the only examples of this. Even the EU is embarking on ambitious plans to wean itself away from monopolistic American tech companies with a European data economy and is actively seeking leadership in the field of AI. Thus, great powers of the near future may end up lurking behind firewalls, jealously guarding the data of their own citizens and being scared of each other’s digital networks, which would be condemned to a perpetual race to develop faster and more efficient data cycles.

/끝/

저자 소개

다니엘 코놀리 교수는 현재 고려대학교 국제대학원에서 연구교수로 재직 중이다. 주요 강의 및 연구분야는 국제관계사, 안보연구 및 기술정치(technopolitics) 등이며, 최근 논문으로 “The Human Security Implications of the Fourth Industrial Revolution in East Asia” (*Asian Perspective*, forthcoming) and “New Rules for New Tools? Exploitative and Productive Lawfare in the Case of Unpiloted Aircraft” (*Alternative*s, March 2019)가 있다.(Email: danielc@korea.ac.kr)

Daniel Connolly is Research Professor at the Graduate School of International Studies, Korea University. His research and teaching interests include the history of international relations, security studies, and technopolitics. His recent publications include “The Human Security Implications of the Fourth Industrial Revolution in East Asia” (*Asian Perspective*, forthcoming) and “New Rules for New Tools? Exploitative and Productive Lawfare in the Case of Unpiloted Aircraft” (*Alternative*s, March 2019).