Cyber Power and The Return of Major War

https://www.e-ir.info/2018/12/12/cyber-power-and-the-return-of-major-war/

STEPHEN PADUANO, DEC 12 2018

In 1998, Michael Mandelbaum declared major war to be obsolete. “The great chess game of international politics is finished,” he announced, and the rising costs and falling gains of conflict have made it unlikely to return. What’s more, Mandelbaum celebrated, a new social stigmatization of war was beginning to lock in the “debellicization” of the world. However, in the final pages of the essay, Mandelbaum concedes, “Currently unforeseen causes of conflict may lurk over the horizon.” He continues, “What lies beyond that horizon, located a decade or two hence, is unknown.” It has now been two decades since the publication of “Is Major War Obsolete?” and a new story must be told. The costs of war have not risen, the gains of war have not fallen, the legitimacy of war has not faded, and major war is neither obsolete nor obsolescent. Indeed, major war is already here. In this article, I will explore the return of major war particularly in the context of cyber warfare. First, I will argue that the costs of going to war are not as prohibitively expensive as Mandelbaum considered them to be. Second, I will demonstrate how the gains of war have meaningfully increased in the contemporary period. Before I begin, however, I must say a word about how major wars begin.

Outbreak

To rationalize war is to say, as Mandelbaum does, that the benefits must outweigh the costs in order for a state to raise an army. This answer feels good because it translates the complex dynamics of war and peace into simple arithmetic. However, rationalizing war has its analytical limits. History is littered with the undesirable wars that defy Mandelbaum’s equation, and any major war would necessarily fall into that camp. Mandelbaum suggests that he is aware of the irrationality of war when he writes of the “Sarajevos of the twenty-first century.”[1] The mention of Sarajevo is meant to warn the reader of the role that accident plays. Just as the assassination of the archduke triggered the unwanted First World War, Mandelbaum says, an accident along the Russian-Ukrainian border, on the Crimean Peninsula, or in the South China Sea could trigger an unthinkable major war today. This tangent of Mandelbaum’s essay has aged well, but it was ultimately just a tangent. Mandelbaum’s thesis remained that in the post-Cold War era, the costs are too high and the benefits are too low. He did not pay enough attention to Sarajevo.

It is important to think of the outbreak of major power war in terms of accidents and not arithmetic. A nuclear war will not start as a nuclear war. It will start as a scare tactic in Eastern Europe, a patrolling mission in the Pacific, a greedy ploy in cyberspace. Mandelbaum asked and answered the wrong question: *should a major power nuke another major power?* Not since the Second World War has the answer been *yes*— and even still, only 34% of Americans believe the United States should have dropped the atomic bomb.[2] The proper question is whether Sarajevos exist. And indeed they do.

Today, the threat of accidents is only growing and the potential theaters of accident – the Sarajevos – are growing as well. An accident in Ukraine, the Baltics, the Baltic Sea, the Black Sea, Syria, the South China Sea, the Korean Peninsula, or cyberspace could trigger a war that defies all advisable calculations. I will consider in particular the consequences of cyberspace, the zone which is the most fraught with danger for the United States, Russia, and China because of the immense vulnerability of those nations’ military, political, and economic interests.

Mandelbaum was wrong to say that if the costs outweigh the benefits then nuclear war will not come about. It was a gross rationalization of the dynamics of war and it overlooked the possibility of accidents and the principle of

escalation. Accidents and escalation are the ingredients of major war, and it is not difficult to conceive of how they might arise today. However, Mandelbaum was right to say that if the benefits outweigh the costs then war is more likely. It is an unfortunate reality though that in cyberspace the benefits of hostile activities are increasingly coming to outweigh the costs, and that the probability of escalation to major war has therefore grown in the past two decades.

Costs

Traditionally, one might think of costs as the financial resources required to organize and execute a policy. In this sense, a nuclear arsenal is quite expensive whereas a cyber arsenal is quite cheap. North Korea currently commits about twenty-five percent of its annual GDP to developing rudimentary nuclear capabilities, a cost that brings with it chronic food shortages and power outages.[3] Its cyber capabilities, however, are threatening to even the most powerful states and require only the cheap costs of widely available education and hardware. However, the real cost of nuclear war for North Korea is a matter of nuclear reprisal. In this sense, the costs of a military action are not offensive but defensive. In cyberspace, the defensive costs of cyber deterrence and reprisals hardly exist.

In his 2014 book *World Order*, Henry Kissinger implored, "A new world of deterrence theory and strategic doctrine now in its infancy require urgent elaboration."[4] This call for theoretical and operational attention, however, has been largely unmet. In the four years since the book was published, Chinese hackers infiltrated the United States' Office of Personnel Management, North Korea crippled Sony Pictures, and Russia breached the servers of the DNC and numerous American polling stations.[5] None of these acts of espionage and destruction – *acts of war* as they would be called in any prior century – has received a proportional and deterring response. The unfortunate reality is that there is no viable theory of cyber deterrence in existence. This is to say, there is no clear threat of retributive costs for launching a cyber-attack.

In *The Virtual Weapon and International Order*, Lucas Kello sought to fill the theoretical lacuna of cyber deterrence with his own theory of "punctuated deterrence."[6] In Kello's view, a state should understand cyber-attacks not as individual episodes but as cumulative actions.[7] A state would employ "a graduated scheme in which penalties are meted out over time and at a moment of the defender's choosing."[8] Kello's theory certainly has its merits. Given the "sub-threshold" insignificance of some cyber-attacks and the bureaucratic difficulty of organizing and executing frequent reprisals, a traditional theory of deterrence that sees each instance of hostility as something to be deterred is bound for failure.

However, the theory's shortcomings are in even greater supply. First, deterrence relies in large part on signalling: it is important that the adversary understand the consequences of his actions. In a regime of punctuated deterrence, where five cyber attacks are permissible but six means war, there is a catastrophic absence of communication. Kello himself notes (prior to proposing his theory): "Each failure to punish increases the willingness to strike again. Inaction, therefore, creates pressures of conflict."[9] In addition to failing to address this problem, punctuated deterrence makes it all the more confusing. Second, Kello's failure to explain the relationship between kinetic and non-kinetic warfare leaves his theory without a principle of proportionality: it remains uncertain when a non-kinetic act of aggression might warrant a kinetic use of force, and to what degree. This becomes particularly salient for our purposes in considering how wars may escalate beyond the cyber plane. Such uncertainty, Kissinger feared three years earlier, would make escalation all the more likely.[10] Third, there continues to exist a "sovereignty gap," as Kello calls it, in which the state is no longer the primary actor in times of war.[11] It is neither the most likely to be a victim of foreign aggression nor is it the most likely to provide defence against foreign aggression. Although Kello details the problems of the sovereignty gap in his book, the issue remains unresolved in his theory. Fourth, obscured attack signatures and networked vulnerabilities – two non-theoretical components of cyber warfare – make deterrence near impossible. If a state does not know who launched an attack (as was the case this summer in Ukraine) and if a state cannot launch a cyber-attack without risking damage to itself or allies (as was the case in 2003 when the United States called off an attack on Iraq's financial systems for fear of crippling Europe's ATM machines), a hostile cyber actor can engage with a much greater level of impunity.[12]

The inadequacies of theories of cyber deterrence leave states undeterred from engaging in the types of hostile behaviors that may provoke an escalation to major war. For all the perils of the Cold War, the certainty and

universality of nuclear deterrence theory provided some element of stability to international politics. In the new cyber era, no such stability exists. This condition is exacerbated by the soaring benefits of cyber warfare.

Benefits

A nation leads a double life online with double the vulnerabilities. As economies, militaries, and political dialogues have joined the digital age, the opportunities for foreign exploitation have grown. This has been done with devastating effect and remarkable success continuously throughout the past two decades. The most beneficial offensive cyber activities to date have been intellectual property theft, in which one country steals the technologies and trade secrets of another country; surveillance and destruction, in which cyber becomes an extension of the traditional role of the military; and political manipulation, in which a state's political landscape is influenced by foreign actors. With the Chinese purloining of American assets, the American attack on Iran's nuclear reactors, and the Russian disinformation campaign against the West, we can see clearly the unrivalled advantages of cyber warfare.

Intellectual property theft costs the United States six hundred billion dollars per year.[13] But what has been far worse is the appropriation of knowledge and capabilities that takes place on the web every day. The Thucydidean rise of China and fall of the United States is in large part hastened by China's cyber exploitation of America's private sector. The competitive advantage that China is gaining against the United States due to intellectual property theft cannot be overstated: it has been an active policy of the Chinese government to facilitate its core private industries by illegally retrieving advantageous information from the United States.[14] It should be no surprise if, in ten years hence, the Chinese cyber-attack on U.S. Steel's research and development arm, hacking of Apple's iCloud servers, and exfiltration of the F-35 designs help produce an industrial sector, tech sector, and defence sector in China that rivals those of the United States.[15] The financial and competitive benefits of hostile engagement have indeed grown in the cyber era.

An increasingly devastating benefit is also the ease of military operations. The most notable to date has been the Stuxnet virus that the United States deployed against Iran's nuclear reactors in 2010. In her tell-all book*Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* , Kim Zetter details the United States' cyber-attack against the Natanz nuclear facilities.[16] She chronicles the ruthless and remarkable efficiency of the virus as it debilitated a system that was "air-gapped," disconnected from the Internet, having a level of security that was widely considered to be impenetrable.[17] However, the most remarkable story of the book is the one that is not told: there would never be a kinetic attack on Natanz. Cyber warfare's appeal, particularly in a case like degrading the technological capabilities of an adversary, is its effectiveness. Stuxnet achieved what only an airstrike could have achieved— provided the jets made it past Iran's missile defence systems, around the turrets stationed outside the nuclear facilities, and away from the jets that Iran surely would have scrambled.[18] In other words, cyber weapons offer the benefit of reliability that physical weapons often cannot.

Even still, the most damning effect of cyber warfare has not been in the economic or military plane— despite the hundreds of billions of dollars lost and the nuclear politics disturbed. Cyber warfare has proven most powerful in the political plane, as the Russian Federation has made clear through multiple information warfare campaigns in the past two years. The NATO handbook on Russian information warfare creates the distinction between *technical* and *psychological* information warfare.[19] The former relates to the hacking, leaking, and spreading of unsavoury or fake information online. Examples of this include the Russian attacks on the DNC's servers, John Podesta's emails, and the Macron Campaign's digital systems.[20] It also includes the rise of "troll armies" that can hijack the public's attention through the creation and amplification of fake news across social media platforms.[21] The latter, psychological information warfare, relates to the content of the information and its ability to divide and distract a population.[22] Taken together, technical and psychological information warfare constitute a desirable new application of non-kinetic warfare that allows a state to steer news cycles, disrupt political agendas, and delegitimize political institutions. Information warfare offers a depth of power that bombs and bullets can hardly achieve: the manipulation of a nation, its values, and its interests. President Trump's fake news-fueled victory, the sun setting of sanctions against Russia, the twenty-five point difference of opinion on Vladimir Putin between Democrats and Republicans, and a record low favorability of democracy and democratic elections show all too well the benefits of information warfare and its likelihood to continue.[23]

Conclusion

Mandelbaum's essay sets out from the observation that the costs of nuclear war are too high and the benefits too low. However, this has always been the case and it has never been the basis for thinking about the outbreak of major war. The question is whether states are engaged in the type of adversarial, accident-prone behaviour that can produce escalation to major war. In cyberspace, this behaviour is in abundance.

In this article, I have shown that the costs of hostile cyber activities are low and the benefits are high. Without a working theory of cyber deterrence and with the many benefits of cyber exploitation, the major powers will continue to push each other towards major war. In certain respects, considering the frequency and intensity of cyber-attacks between the major powers today, we are already well on our way there. Although this activity has not yet met Mandelbaum's conception of "major war," it has nevertheless made Sarajevo far more likely to come about. Major war is, therefore, neither obsolete nor obsolescent— it is on the rise.

Notes

[1] Mandelbaum, 31.

[2] Stokes, Bruce. "70 Years After Hiroshima, Opinions Have Shifted on Use of Atomic Bomb," in*Pew Research Center.* August 4, 2015.

[3] Pearson, James and Ju-Min Park. "North Korea overcomes poverty, sanctions with cut-price nukes," in *Reuters*. January 11, 2016.

[4] Kissinger, 347.

[5] Koerner, Brendan. "Inside the Cyberattack that Shocked the US Government," in *Wired*. October 23, 2016; Boorstin, Julia. "The Sony Hack: One Year Later," in *CNBC.* November 25, 2015;

[6] Kello, 119-159.

[7] Kello, 208-209.

[8] Ibid.

[9] Kello, 206.

[10] Kissinger, Chapter 9.

[11] Kello, 229.

[12] Borys, Christian. "The day a mysterious cyber-attack crippled Ukraine," in *BBC*. July 4, 2017; Kello, 201.

[13] Blair, Dennis and Keith Alexander. "China's Intellectual Property Theft Must Stop," in *The New York Times*. August 15, 2017.

[14] Kuchler, Hannah. "US Charges Three Chinese Nationals Over Hacking," in *The Financial Times*. November 28, 2017.

[15] Elmquist, Sonja. "U.S. Steel Seeking China Import Ban After Alleged Hacking," in *Bloomberg News*. April 27, 2016; Finkle, Jim, Gerry Shih, Ben Blanchard. "China-backed hackers target Apple's iCloud users," in *Reuters*. October 21, 2014; Ling, Justin. "Man Who Sold F-35 Secrets to China Pleads Guilty," in *Vice News*. March 24, 2016.

[16] Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* . Crown Publishers: New York. 2014.

[17] Ibid.

[18] Ibid.

[19] Giles, Keir. *Handbook of Russian Information Warfare*. NATO Defense College (2016). Pp. 9-11.

[20] Lipton, Eric, David Sanger, Scott Shane. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," in *The New York Times*. December 13, 2016; Willsher, Kim and Jon Henley. "Emmanuel Macron's campaign hacked on eve of French election," in *The Guardian*. May 6, 2017.

[21] Shane, Scott. "The Fake Americans Russia Created to Influence the Election," in *The New York Times*. September 7, 2017.

[22] Giles, 9.

[23] Schor, Elana. "White House to Congress: Russia sanctions not needed now," in *Politico*. January 29, 2018; Pew Research Center. "In U.S., Democrats feel more threatened by Russian power." August 15, 2017; Bremmer, Ian. "Is Democracy Essential?" *NBC News*. February 13, 2018.

Sources

Blair, Dennis and Keith Alexander. "China's Intellectual Property Theft Must Stop," in *The New York Times*. August 15, 2017.

Boorstin, Julia. "The Sony Hack: One Year Later," in *CNBC.* November 25, 2015.

Borys, Christian. "The day a mysterious cyber-attack crippled Ukraine," in *BBC*. July 4, 2017; Kello, 201.

Bremmer, Ian. "Is Democracy Essential?" *NBC News*. February 13, 2018.

Elmquist, Sonja. "U.S. Steel Seeking China Import Ban After Alleged Hacking," in *Bloomberg News*. April 27, 2016.

Finkle, Jim, Gerry Shih, Ben Blanchard. "China-backed hackers target Apple's iCloud users," in *Reuters*. October 21, 2014.

Giles, Keir. *Handbook of Russian Information Warfare*. NATO Defense College. 2016.

Kello, Lucas. *The Virtual Weapon and International Order*. Yale University Press. 2017.

Kissinger, Henry. *World Order*. Chapter 9: "Technology, Equilibrium, and Human Consciousness." Penguin Press. 2014.

Koerner, Brendan. "Inside the Cyberattack that Shocked the US Government," in *Wired*. October 23, 2016.

Kuchler, Hannah. "US Charges Three Chinese Nationals Over Hacking," in *The Financial Times*. November 28, 2017.

Ling, Justin. "Man Who Sold F-35 Secrets to China Pleads Guilty," in *Vice News*. March 24, 2016.

Lipton, Eric, David Sanger, Scott Shane. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," in*The*

New York Times. December 13, 2016.

Mandelbaum, Michael. “Is Major War Obsolete?” in *Survival*, Vol. 40, No. 4, 1998-1999. Pp. 20-38.

Pearson, James and Ju-Min Park. “North Korea overcomes poverty, sanctions with cut-price nukes,” in *Reuters*. January 11, 2016.

Pew Research Center. “In U.S., Democrats feel more threatened by Russian power.” August 15, 2017.

Schor, Elana. “White House to Congress: Russia sanctions not needed now,” in *Politico*. January 29, 2018.

Shane, Scott. “The Fake Americans Russia Created to Influence the Election,” in *The New York Times*. September 7, 2017.

Stokes, Bruce. “70 Years After Hiroshima, Opinions Have Shifted on Use of Atomic Bomb,” in*Pew Research Center.* August 4, 2015.

Willsher, Kim and Jon Henley. “Emmanuel Macron’s campaign hacked on eve of French election,” in *The Guardian*. May 6, 2017.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon* . Crown Publishers: New York. 2014.

About the author:

Stephen Paduano is an Associate at the IDEAS Institute of the London School of Economics. His writing and research focus on British and American politics, as well as liberal political theory. He is a regular contributor to Foreign Policy and has appeared on CNN and Sky News. Previously, he was a staffer to Hillary Clinton on her 2016 presidential campaign. He holds a bachelor’s with honors from Stanford University and a master’s with distinction from the London School of Economics.