Cyber Does Not Transform International Security and War: Understanding Cyber through Existing Theoretical Tools in International Relations

Jun Kyu Baek

Graduate student at the Yonsei Graduate School of International Studies

Though it may be understandable to view cyber and information technology as disruptive and even transformative for a wide range of domains of modern civilization, this preconception doesn't necessarily apply in the context of international security and war. This essay argues that the advent of cyber does not fundamentally transform security and war; it reasons that cyber has not shifted the fundamental goals of security nor the reasons why wars are fought. The essay first looks at the literature on international relations and cybersecurity to synthesize three propositions supporting the counter-position that cyber transforms security and war. After evaluating these three propositions in turn, the essay finds them all to be debatable and inconclusive. Having thusly contended that international security yet remains untransformed by cyber, the essay subsequently demonstrates that it is possible to understand cyber in international security via theories used for traditional security affairs. An alternative explanation of cyber in international security is subsequently provided, where existing conceptual tools in international relations—such as information warfare, the offense-defense balance, and deterrence theory—are utilized both to account for the use of cyber in international security and to show that cyber is not so transformative that it precludes the use of existing theories in international security. Cyber may change how wars are fought, but not why they are fought, and can therefore still be interpreted using traditional conceptual tools.

1. Introduction

While the impact of cyber and information technology can be observed across various domains of modern civilization, a distinction should be made between “change” and “transformation”. [1] This distinction asks if cyber is so fundamentally disruptive that existing modes of thought will be unrecognizably altered, or whether traditional paradigms can even be applied in the age of cyber. This essay responds to these questions by examining the impact of cyber over a subdomain of international relations: international security and war.

Explaining *why* wars are waged—or, in other words, the causes of war and the logic underlying international security—is a lengthy discussion separate from the focus and scope of this essay. Given the issues this essay seeks to address and for the sake of brevity and convenience, the essay will utilize abstractions such as “politics”, “policy”, and the pursuit of “survival”, “security”, or “the national interest” within the uncertain environmental conditions of international politics, as shorthand to explain away the reasons why international actors sometimes elect to wage war.

Utilizing this language, this essay argues that cyber will not transform international security and war, holding that cyber does not significantly alter the underlying, fundamental policy/strategic goals of security and war. Though cyber may change *how* wars are fought, it is unlikely to transform the fundamental reasons *why* they are fought. Since these underlying reasons remain unchanged, it is feasible to incorporate cyber into existing tools and paradigms for understanding security and war.

To develop this argument, this essay will first critique common propositions suggesting that cyber will “transform” security and war. Each of these propositions are found to be implausible, which suggests that security and war have not been transformed by cyber. Building upon the argument that security and war have remained fundamentally unchanged, the second part of the essay will describe how to validly incorporate cyber into existing tools and concepts for understanding security and war.

[1] “The Impact of Digital Technologies”, United Nations, https://www.un.org/en/un75/impact-digital-technologies; Martin Mühleisen, “The Long and Short of The Digital Revolution”, *Finance & Development* 55, no. 2 (June 2018): pp.4-8; Charles Weiss, “How Do Science and Technology Affect International Affairs?” *Minerva* 54 (2015): pp. 411-430.

2. Not Very Transformational

To transform security and war, cyber should irrevocably alter their policy and strategic dimensions. In doing so, cyber must buck existing tools and paradigms used to understand security and war.[2] It is insufficient to point to the altered methods or novel expressions of warfare as evidence of transformation. Rather, this essay presupposes that real transformation occurs when leaders alter how they think about security, or when the underlying political and strategic drivers of war have been changed. [3]

In this section, the essay will illustrate how cyber lacks such transformative qualities. First, the essay will critique the extent to which cyber should be conceptualized as a goal versus a means through which larger strategic goals are achieved. Second, the essay will review the basic defining traits of cyber as it relates to international security affairs. These traits will be used to synthesize and then evaluate three commonly-held beliefs about cyber's ostensibly transformative impact on international security and war.

2.1. A New Way of Warfighting?

Increasing concerns about the role, utility, and risks of cyber in war have intensified the call to operationalize cyber as its own distinct military domain, alongside land, sea, air, and space. US Cyber Command (USCYBERCOM) actively conceptualizes cyberspace as the fifth operational domain of the

[2] To illustrate, Thomas Rid writes that to be classified as "war", an act must fulfill three criteria: it must be violent (i.e., lethal), coercive (i.e., must intend on bending the adversary to one's will), and political (i.e., war is always motivated by political purposes). See Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies* 35, no. 1 (2012): pp. 7-10.

[3] Examples of novel expressions of so-called "cyberwarfare" can include zero-day cyber-physical attacks, cyber-espionage, cyber terrorism, and cyber information warfare.

military, a domain in which USCYBERCOM strives to achieve dominance.[4] USCYBERCOM no longer believes it is sufficient to treat cyber as merely an asset—superiority in the cyber-realm is the goal, and attaining it may require new kinds of capabilities,[5] innovations, and concepts.[6] Here, the claim is made that cyber has somehow meaningfully changed security and war, to such an extent that the US military now pursues unique distinct capabilities

[4] USCYBERCOM specifies cyberspace superiority 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 forces at a given time and place without prohibitive interference by an adversary". USCYBERCOM's view of cyber as a distinct domain is also apparent in how it vows to attain superiority through persistent and forward-pushing (as opposed to reactive and singular) engagement in cyberspace: "Cyberspace persistence is the continuous ability to anticipate the adversary's vulnerabilities, and formulate and execute cyberspace operations to contest adversary courses of action under determined conditions". See United States Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, (April 2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf, pp. 6. For more on the US' operationalization of cyber as a military domain, see Jacquelyn G. Schneider, et al., "Ten Years In: Implementing Strategic Approaches to Cyberspace", pp. 5-6. For more on cyber persistence theory, see Michael P. Fischerkeller and Richard J. Harknett, "Cyber Persistence Theory, Intelligence Contests and Strategic Competition", Institute for Defense Analysis, (June 2020): pp. 1-11.

[5] For example, capabilities like boots-on-the-ground soldiers may prove less important than computer-savvy cyber specialists when pursuing superiority in the cyber domain. Building these capabilities requires policies that nurture and attract the relevant talent (e.g., policies that improve technical education and linkages with civilian groups at the forefront of the technology industry), as opposed to policies that help train a less-useful traditional soldiery. Indeed, the NATO Industry Cyber Partnership (NICP) has worked since 2014 to bolster civilian-military cooperation in the cyber domain through the exchange of best practices, review of NATO's cyber-exercises, and sharing of information about new or upcoming innovations. See Jamie Shea, "Cyberspace as a Domain of Operations: What is NATO's Vision and Strategy?", pp. 147-148.

[6] For example, NATO views cyber as an operational domain of war and a paradigm-breaking force due to its unprecedented capacity to induce volatility. This view stems from cyber's ability to achieve desirable outcomes with relative ambiguity, frequency, and rapidity compared to conventional means; to disrupt state control over once-secure processes such as elections, critical infrastructure, economy, etc.; its availability to a wide range of actors; and other such distinctive characteristics. The volatility of cyber has spurred NATO to reshape its organization, policies, and resources to better prepare for aggression and defense in cyberspace. Ibid, pp. 140-141, 148-149.

and stratagems to thrive in a discrete domain of military-cyber affairs.

This claim is problematic firstly because the pursuit of "cyber-superiority" can be simply envisaged as a new way of achieving the unchanged, underlying policy goals of war. Superiority over the cyber domain is a valuable goal, not necessarily because it galvanizes the military towards the goal of superiority, but because cyber-superiority serves the larger policy and strategic goals of the national interest. While cyber-superiority admittedly represents a novel method of achieving said policy goals, there is little to suggest that the logic that drives politics and policy itself have changed,[7] nor is there much strategic validity in treating cyber operations as an end unto itself.[8] Put in other words, cyber has not affected the security/self-help logic that guides policy/strategic decisions. Building up cyber capabilities to better compete in the cyber domain may be a novel expression of that underlying logic, but does not equate to having transformed it.

Furthermore, even if cyber capabilities are a novel means of achieving the policy goals of war, conventional means are still necessary to achieve those goals. Cyber has not supplanted or substituted conventional forces. Rather, cyber is often used as a force multiplier or a complement to existing, conventional means—all of which are utilized to achieve strategic ends.[9] In

[7] USCYBERCOM states that its goal of attaining attain cyber-superiority is rooted in the desire to "defend [US] interests and protect [US] values… to improve security and stability". In other words, cyber-superiority is not viewed as USCYBERCOM's end-goal. (See United States Cyber Command, Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command, pp. 2.) Second, NATO's emphasis on cyber is predicated on the belief that cyber will help it fulfill its function as a collective security pact between 30 different nation-states – an agreement maintained out of the participants' goal of maximizing national security. As long as the operationalization of cyber is driven by the enduring strategic goal of maximizing national security, then one cannot say that the operationalization of cyber has transformed war. See: Jamie Shea, "Cyberspace as a Domain of Operations: What is NATO's Vision and Strategy?", pp.133-134 and North Atlantic Treaty Organization, "Cyber Defense Pledge", press release, July 8, 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

[8] John Sheldon makes the latter point clear. See John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War", pp. 102-103.

[9] John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War", pp. 99-100; P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, (New York: Oxford University Press, 2014), pp. 128-132, 146.

war, a strategic effect—that which has meaningful consequences for policy—is achieved via coercion, which is easiest with the application of conventional kinetic force (e.g. the destruction of enemy forces or occupation of strategically important territories). The reason for this is simply because international actors live in a three-dimensional physical space. Coercion is most effective when survival is threatened, and survival is best threatened when the threats are physical, present, and existential. Cyber, on the other hand, does not coerce on its own but *facilitates* coercive physical actions, such as by disabling the cyber-based command-and-control systems that coordinate physical attacks.[10]

An example of this is Operation Orchard, when Israel hacked into the Syrian air defense network and fed it false images. This prevented the Syrian radar from detecting the Israeli air-fighters sneaking into Syrian airspace, which facilitated Israel's bombing of the Syrian nuclear complex at Al-Kibar.[11] This example illustrates cyber's value as a complement to conventional force and its limited ability to achieve strategic effects on its own, rather, it was the conventional Israeli bombers that outputted the coercive strategic effect. Conventional weapons yet retain their primacy in war, and thus, cyber may not be as transformative for war as believed.[12]

2.2. Cyber: Basic Traits

Cyber is characterized by traits that are commonly believed to be destabilizing. These traits are claimed to be transformative for war and international security by allegedly introducing unprecedented levels of instability in inter-state security affairs. These cyber-defining traits

[10] John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War", pp. 99.

[11] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, pp. 126-127.

[12] A potential counterargument to this point presents itself in the advent of *kinetic* cyberweapons (cyber assets as seen in the Stuxnet incident that can inflict physical damage). This view holds that, if cyberweapons like Stuxnet can inflict serious kinetic damage, then cyber can achieve strategic effects and will thus revolutionize war and security. However, even with the damage inflicted by Stuxnet upon Iranian centrifuges, Stuxnet was ultimately unable to coerce the Iranians into shutting down their nuclear program. This casts doubt on the ability of kinetic cyberweapons to independently achieve strategic effects, and therefore, its potential to revolutionize war and security.

are established in this essay as ambiguity, availability, and plasticity.

First, cyber is *ambiguous* in the sense that it is inherently difficult to identify the perpetrators of cyberattacks. The fact that the majority of major cyberattacks up until 2010 have been unattributed serves to reinforce this point.[13]

Cyber is also widely *available* and ubiquitous. Logically, the more wired a country and its individuals are, the more vulnerable they are to cyberattacks and malware. As information technologies proliferate, cyberweapons become increasingly available to a larger number of actors and can be used to attack a greater number of increasingly "wired" targets. This is compounded by the relatively low costs of entry for cyberattacks (i.e., the costs of learning how to conduct cyberattacks or how to use malware). For example, Skygrabber, the software that was used by Iraqi insurgents in 2009 to hack into and spy on the digital video feeds of US drones, was available to download online for as cheap as USD $29.95. Such relatively low entry barriers make cyberweapons available to a larger number of actors in an increasingly digitally interconnected, and thus target-rich, environment.[14]

Finally, cyber is *plastic,* meaning that it can fulfill multiple purposes. The multifaceted, fungible, and viral qualities of cyber mean that it is difficult to manage perceptions and expectations regarding cyber-intrusions. In other

[13] Eric Talbot Jensen, "Cyber Deterrence", *Emory International Law Review* 26, no. 2 (2012): pp. 785-787. The problem of attribution compounds when considering the non-geographic nature of cyber, which enables (potentially) any cyber-actor to perpetrate cyberattacks on anyone or anything, anywhere in the world. The ambiguity inherent to cyber not only explains why actors (particularly weaker actors that face conventionally stronger opponents) are attracted to the use of cyber, but also creates an "attribution dilemma" for victims of cyberattacks, where the benefits of casting blame on an ambiguous perpetrator must be weighed against the political downsides of doing so. See: Stephen Blank, "Web War I: Is Europe's First Information War a New Kind of War?" *Comparative Strategy* 27, no. 3 (2008): pp. 241; John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War", *Strategic Studies Quarterly* 5, no. 2, (Summer 2011): pp. 99-101; and P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), pp. 72-76, 145-146.

[14] Siobhan Gorman, Yochi J. Dreazen, and August Cole, "Insurgents Hack U.S. Drones", *Wall Street Journal*, December 17, 2009, https://www.wsj.com/articles/SB126102247889095011; P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, pp. 150-153; and John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War", pp. 97-98.

words, it is difficult to determine whether a cyberattack should be treated as a relatively inoffensive transgression or a deliberate, meaningful provocation. This makes it difficult to predict how victims of a cyberattack might respond, as demonstrated during the 2017 NotPetya ransomware attack. Initially afflicting Ukrainian organizations via Ukrainian tax-filing software, the NotPetya virus quickly spread across Europe and the US. With the damage adding up to an estimated $53 billion, the US and the UK blamed Russia for the attack and called for international sanctions.[15] While it is difficult to fully know Russia's intentions behind the cyberattack, assuming that Russia was indeed the perpetrator, it is unlikely that Russia deliberately set out to directly antagonize the US, Germany, France, and other major European stakeholders and incur their collective wrath. It is more plausible to think that the attack was intended to harm Ukraine, but unintentionally spread to Europe and the US.[16] Here, the plastic nature of cyber is illustrated. The NotPetya cyberattack unexpectedly went beyond its intended target and triggered unexpected and undesirable responses from others. This shows the difficulty of controlling the effects of cyberattacks and managing perceptions and expectations in cyber.

[15] Jamie Shea, "Cyberspace as a Domain of Operations: What is NATO's Vision and Strategy?", *MCU Journal* 9, no. 2 (Fall 2018): pp. 139; Suzanne Barlyn, "Global cyber attack could spur $53 billion in losses: Lloyd's of London", *Reuters*, July 17, 2017, https://www.reuters.com/article/us-cyber-lloyds-report-idUSKBN1A20AB; "Global ransomware attack causes turmoil", *BBC News*, June 28, 2017, https://www.bbc.com/news/technology-40416611; and "UK and US blame Russia for 'malicious' NotPetya cyber-attack", *BBC News*, February 15, 2018, https://www.bbc.com/news/uk-politics-43062113.

[16] Several facts about the 2017 NotPetya cyberattack reflect the likelihood that the attack was primarily intended to affect Ukraine, and likely only Ukraine. First, the attack coincided on Ukraine's Constitution Day on June 28; second, 80% of all systems infected by the NotPetya malware were in Ukraine; and finally, the cyberattack took place amidst the backdrop of ongoing conflict between Ukraine and Russia. Jane Wakefield, "Tax software blame for cyber-attack spread", *BBC News*, June 28, 2017, https://www.bbc.com/news/technology-40428967; Ellen Nakashima, "Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes", *The Washington Post*, January 12, 2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

2.3. Unprecedented Instability?

The above traits combine to create three general beliefs about the destabilizing impact of cyber in security-military affairs. These beliefs conceive cyber as a common source of instability and of engendering more inter-state conflict and war. In short order, the three propositions are that cyber favors and enables military/strategic offense over military/strategic defense, that cyber emboldens and empowers conventionally weaker states to engage in asymmetric warfare, and that the cyber-attribution dilemma undermines deterrence and therefore stability.[17]

The first of these beliefs holds that cyber will shift the offense-defense balance to irrevocably favor the offense.[18] Here, it is argued that cyber incentivizes persistent cyberattacks due to cyber's relatively lower barriers to entry, the ability to accrue gains irrespective of geography and physical limitations, the ambiguity of cyber-attribution (and thus the theoretically reduced risk of facing retaliation), and the strategic ineffectiveness of cyber-defenses.[19]

Though the offense-favoring nature of cyber has been argued to be transformative for war and security, the dominance of the offense is not historically abnormal, nor does it always generate instability. The Napoleonic

[17] "The emerging literature on the Cyber Revolution is uneven, but three widely held beliefs can be identified. Together these can be taken as a thesis that critical economic and military infrastructure is dangerously vulnerable because the internet gives militarily weaker actors asymmetric advantages, offense is becoming easier while defense is growing harder, and the difficulty of attributing the attacker's identity undermines deterrence." John R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies* 22, no. 3 (2013): pp. 369.

[18] According to the offense-defense balance, war is more likely when the offense is advantaged, and conquest is made easy; war is less likely when the defense is favored, and conquest is difficult. The notion that cyber advantages the offense therefore implies that cyber is more conducive to war and instability. See: Stephen Van Evera, "Offense, Defense, and the Causes of War", *International Security* 22, no. 4 (Spring 1998): pp. 5-6; John R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", pp. 375-377; P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, pp. 154.

[19] Jacquelyn G. Schneider, et al., "Ten Years In: Implementing Strategic Approaches to Cyberspace", *Newport Papers* 45, (2020): pp. 48-49. Indeed, the US Air Force's 2014 budget shows that it spent 2.4 times as much on cyber offense research as compared to cyber defense. See W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, pp. 137.

Wars were characterized by offense dominance, and yet the decades following them were peaceful despite no clear evidence of military innovations that might have shifted the balance towards the defense, therefore making it difficult to say that offense-dominance regularly leads to conflict.[20] Crucially however, shifts in the offense-defense balance do not change the underlying political and strategic drivers of war. Generally speaking, Napoleonic France's invasion of Europe was the result of the desire to maintain and expand its power in the face of a competitive European geopolitical environment.[21] Here, the political or strategic goals that might have initiated the Napoleonic Wars were informed less by the offensive/defensive character of the military technologies of the time, and more by abstract yet fundamental notions of the national interest, security, and survival. Shifts in the offense-defense balance do not necessarily overshadow this fundamental driver of geopolitics. Likewise, the belief that cyber shifts the balance in favor of the offense does not transform the underlying logic of war and security.

Second, there is the belief that the asymmetrical nature of cyber empowers weaker states against stronger states, thus leveling the playing field across international politics.[22] Weaker states (states with weaker *conventional* capabilities than others) may find it cheaper and easier to adopt cyberweapons than conventional weapons due to the relatively lower entry barrier of cyberweapons. Such cyberweapons provide weaker states with the means with which to conduct asymmetric warfare against conventionally-powerful rivals. Cyberweapons provide certain strategic advantages for weaker countries, such as allowing them to launch attacks from a position of relative safety (due to the aforementioned problem of identifying the perpetrators of cyber-attacks). Cyber also provides weaker states with a more target-rich environment consisting of powerful states increasingly dependent on digital infrastructure for their prosperity. As a result, weaker actors empowered by cyberweapons would pose more of a threat to

[20] James D. Fearon, "The Offense-Defense Balance and War Since 1968" (unpublished manuscript, April 8, 1997): pp. 29-30.

[21] Gunter E. Rothenberg, "The Origins, Causes, and Extension of the Wars of the French Revolution and Napoleon", *Journal of Interdisciplinary History* 18, no. 4 (Spring 1988): pp. 771-772.

[22] John R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", pp. 375.

conventionally strong actors, thus raising instability in inter-state affairs.[23]

Yet, stating that cyber mostly favors weaker actors and asymmetric warfare is debatable. Kinetic cyberweapons like Stuxnet feature high barriers to success that could only have been surmounted by powerful actors such as the United States. The attention that Stuxnet-level cyberattacks can attract can also be undesirable for conventionally weaker actors. As such, while low-level cyber-irritants are admittedly profuse, [24] cyberweapons can also compound the already formidable strength of the strong as opposed to unilaterally favoring the weak.[25] But more importantly, the question of whether cyber favors the weak or the strong does little in changing the fundamental drivers of war and security. Cyber little changes the fact that a state, regardless of its strength, will tend to respond to its political and strategic environment with whatever available means. The main thing that changes with the introduction of cyber is the probability of cyber operations being selected as the policy tool of choice. Cyber does little to change the underlying logic generating these policy responses in the first place.

Finally, deterrence theory can be seen as inapplicable to cyber due to difficulties with attribution in cyber, the limited utility of cyber-defense and cyber-retaliation strategies, and how deterrence in cyber is undermined rather than facilitated by the signaling of one's awareness of an adversary's actions.[26] Rather than deterring adversaries which promote stability by disincentivizing aggression, cyber triggers destabilizing security dilemmas in the form of cyber arms races.[27] To make deterrence work in a traditional context, credible and guaranteed threats must be clearly signaled to known threatening actors;

[23] Weaker actors can be advantaged when considering how less ”wired” they are compared to stronger actors. Former NSA expert Charlie Miller claimed in 2011 that North Korea would need only three years and $50 million to defeat the US in a cyberwar. Part of this claim was made on the basis of North Korea's lack of digital infrastructure, and thus fewer vulnerabilities, compared to the US. Mark Clayton, “The Cyber Arms Race”, *The Christian Science Monitor*, March 7, 2011, https://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race.

[24] “Script kiddie” DDoS attacks being one example.

[25] John R. Lindsay, “Stuxnet and the Limits of Cyber Warfare”, pp. 385-389.

[26] Taddeo explores the problems of applying deterrence theory to cyberspace on these grounds. See Mariarosaria Taddeo, “The Limits of Deterrence Theory in Cyberspace”, *Philosophy & Technology* 31 (2018): pp. 343-352.

[27] John R. Lindsay, “Stuxnet and the Limits of Cyber Warfare”, pp. 376-377.

almost none of these requirements are met in cyberspace.[28] Instead of deterrence, the persistence and offense-advantaged nature of cyberattacks would encourage actors to engage in cyber arms races with their rivals, thus leading to instability.[29]

The Stuxnet incident in the context of U.S.-Iranian relations may be interpreted either as a failure or a success of cyber-deterrence. On the one hand, Stuxnet may be viewed as an example of how deterrence is inapplicable to cyber, as the U.S. was able to escape culpability for at least a year after launching their virus. It also seems that once evidence of the U.S.' offensive cyber capabilities became apparent, they were unable to deter Iran's alleged cyber-retaliations, which came in the form of alleged Iranian Distributed Denial-of-Service (DDoS) attacks against U.S. banks and the employment of the Shamoon virus against Saudi Aramco in 2012. On the other hand, deterrence may have prevailed in the Stuxnet case, given the restraint practiced by the U.S. and Iran. For the former, the design and execution of Operation Olympic Games (which deployed Stuxnet against Iran) was characterized by caution, uncertainty, and corresponding attempts to limit the damage Stuxnet would inflict. In the case of the latter, Iran's cyber-retaliations in the aftermath of Stuxnet amounted to irritants, constituting modest and unsophisticated attacks that resulted in no real lasting damage or significance.[30]

In any case, it is problematic to argue that cyber necessitates new paradigms for understanding war and security simply because cyber is incompatible with deterrence theory. Either cyber *is* understandable through deterrence frameworks (in which case cyber is understandable through traditional security frameworks, cannot have transformed security, and doesn't necessitate new paradigms for security), or cyber

[28] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, pp. 144-147.

[29] Ibid., 156-162.

[30] For a discussion of how the theoretical notion of cyber-deterrence could pertain to the Stuxnet incident between the U.S. and Iran, see John R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", pp. 397-401.

cannot act as deterrents and will instead initiate arms-race escalation,[31] a concept that also has precedent in traditional security thinking.[32] In either case, existing frameworks can be used to comprehend the use of cyber, which is reflective of how cyber has changed only the superficial aspects of war and security while leaving their fundamental drivers intact.

Overall, it is debatable whether cyber is truly a source of instability. However, it is clear that cyber does not alter the underlying reasons why actors choose to go to war because cyber is offense-dominant, asymmetric, and deterrence-incompatible, which makes it have little bearing on the underlying drivers of war and security thinking.

3. New Tools, Same Game

This essay has thus far established that cyber has *not* changed the fundamental drivers of policy and security, and that the beliefs which hold that cyber is transformational for international security and war are in fact debatable and inconclusive. [33] This suggests that international security and war likewise have not been fundamentally transformed, which would also imply that existing tools for understanding security and war are still viable in a cyber-infused world. This section explores this implication further by demonstrating how cyber can be understood through the use of existing concepts and tools.

[31] A "cyber arms race" is observable in the relationship between the U.S. and China, in which each country is attempting to identify and hoard zero-day vulnerabilities in each other's systems whilst escalating the volume, frequency, coordination, and competence of various kinds of cyberattacks – from phishing to intellectual property theft – against each other. Nicole Perlroth, "How China Transformed Into a Prime Cyber Threat to the U.S.", *The New York Times*, updated July 20, 2021, https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html.

[32] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, pp. 156-162.

[33] These "fundamental drivers" of policy and strategy, as described elsewhere in this essay, can arguably be defined as the pursuit of security within the self-help conditions of international politics. For further reading on what the nature and motivations behind war and security thinking, see: Ivan Briscoe, "Conflict, security and emerging threats", in *Clingendael Strategic Monitor 2014*, ed. by Jan Rood (Clingendael Institute, 2014), pp. 146-147; Jack S. Levy, "The Causes of War and the Conditions of Peace", *Annual Review of Political Science* 1 (1998): pp. 145-151.

Understanding cyber in terms of “information warfare” (IW) provides the first case in point. Information warfare is “the deliberate use of information by one party on an adversary to confuse, mislead, and ultimately to influence the choices and decisions that the adversary makes”.[34] Examples of this include the apocryphal Trojan Horse, the 1870 Ems Telegram incident,[35] the 2007 cyberattacks on Estonia, and Operation Orchard in 2007.[36] While cyber-IW combines cyber with traditional IW to generate new characteristics, cyber-IW remains a tool for achieving policy and strategic goals through deception and influence.[37] The case of Russia’s cyber-IW operations in Georgia in 2008, for example, can be understood as a means of achieving Russia’s overall

[34] Herbert Lin and Jackie Kerr, “On Cyber-Enabled Information/Influence Warfare and Manipulation”, Center for International Security and Cooperation, Working paper, August 2017, pp. 4-5.

[35] The Ems Telegram refers to the incident in 1870 in which Otto von Bismarck of Prussia manufactured a diplomatic crisis between Prussia and France. Bismarck released a statement to the Prussian media that gave off – as was Bismarck’s intention – the impression that the French ambassador was more demanding than he had been to the Prussian king, and the Prussian king more insulting than he had been to the French ambassador. This deception worsened Prussian-French relations and presaged war between the two countries, all as desired by Bismarck.

[36] Thomas Rid argues that cyber-incidents popularly trumpeted as examples of “cyber war” (e.g., the 2007 Estonian cyberattacks, Operation Orchard, Stuxnet, and others) are merely sophisticated examples of old activities in warfare: sabotage, espionage, and subversion. Rid further argues that sabotage, espionage, and subversion are not themselves examples of standalone “war”, and rather, are auxiliary activities for military operations. As such, for Rid, cyber-incidents observed to the present day cannot be called “cyber war”. See Thomas Rid, “Cyber War Will Not Take Place”, pp. 16-29.

[37] New characteristics such as: the rising number of actors willing to utilize cyber-IW due to the ambiguity inherent in cyberoperations; the ease with which cyber-IW operations can be conducted due to the low costs of conducting such operations and the non-geographic nature of cyber; and the relative attractiveness of cyber IW due to the highly-connective (and therefore target-rich and vulnerable) nature of the Internet. See Herbert Lin and Jackie Kerr, “On Cyber-Enabled Information/Influence Warfare and Manipulation”, Center for International Security and Cooperation, pp. 11-14.

goal of occupying the territory previously owned by Georgia.[38] This shows that the Georgia incident does not change the fact that IW, whether traditional or cyber-enabled, serves as an instrument of policy goals. Russia's other cyber-IW operations, such as the cyber operations during the annexation of Crimea in 2014 as well as during the U.S. elections in 2016;[39] are also examples of information warfare being utilized to achieve policy goals.

Another view holds that cyber information warfare is somehow transformative because of the simplicity of conducting information warfare through cyber. This view holds that because the modern world is dependent on Internet hyperconnectivity for its prosperity, the world has become a more vulnerable and target-rich environment wherein people who spread disinformation and agents of psychological warfare can ply their trade. However, this view can also be understood through the concept of offense-defense balance. As explained previously, shifts in the offense-defense balance do not constitute a transformation in security and war. The fact that cyber can be understood in terms of the offense-defense balance demonstrates how cyber can be incorporated into an existing paradigm of war and security.[40]

A final example of how cyber can be understood in terms of existing

[38] Russia's cyberattacks against Georgia disabled Georgian websites, which hampered the government's ability to communicate with the public even as Russian forces invaded the country. The case thus demonstrates cyber as a complement, or force multiplier, for conventional and coercive military force. See David Hollis, "Cyberwar Case Study: Georgia 2008", *Small Wars Journal* (2011): pp. 1-5.

[39] Russia's use of cyber to conduct information warfare is argued to be part of the country's overall strategy to utilize cyber and other "cognitive-psychological forms of influence" to wage a kind of asymmetric, hybrid warfare against conventionally powerful adversaries. Termed the "Gerasimov Doctrine", this strategy underscores how cyber capabilities are viewed as tools in the service of policy/strategy goals – in this case, those goals being Russia's national security in the face of geostrategic and technological challenges. Herbert Lin and Jackie Kerr, "On Cyber-Enabled Information/Influence Warfare and Manipulation", pp. 15-16.

[40] It should also be noted that it is difficult to definitively say that cyber favors the offense. While cyber does possess characteristics that seemingly favor the offense, the defense is by no means helpless in cyber: the presence of "cyber kill chains" can significantly slow down and mitigate the efficacy of cyberattacks, while conventional military or diplomatic tools can be used to deter cyberattacks. See: John R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", pp. 394-395 and P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, pp. 155-156.

theories lies in the debate on whether cyberweapons can be used as stabilizing deterrents or will be used to provoke destabilizing arms races. Since both deterrence theory and arms races are existing frameworks in security and war, cyberweapons can thus be understood through either of these existing frameworks. Determining which side of the debate cyberweapons fall under, deterrence or arms race, is irrelevant for the purposes of this essay's argument. The point this essay makes is that there are existing ideas—ideas grounded on a traditional understanding of security and war—that can be used to theorize about the nature and use of cyberweapons.[41]

These three examples demonstrate the viability of incorporating cyber into existing tools and concepts. Moreover, this compatibility illustrates the nature of "cyber warfare" as just another tool for fulfilling the policies and strategies representing the "national interest".[42] If the national interest is understood as the desire to provide for one's security and interests in the face of environmental uncertainty, then the national interest is less-malleable and less unaffected by the advent of cyber technologies.[43] If so, then cyber warfare, as viewed through the prism of the higher-order political and strategic goals constituting "national interest", may also be understood through or incorporated into already existing concepts used to understand security and war.

4. Conclusion

Carl von Clausewitz once described war as "the continuation of politics by

[41] As insinuated elsewhere in this essay, the debate is ongoing over the question of whether cyber can act as a deterrent or arms-race escalator. For an example of the former, Borghard and Lonergan make the case that cyber can act as a deterrent if properly framed through "deterrence-by-denial" logic. See Erica D. Borghard and Shawn W. Lonergan, "Deterrence by denial in cyberspace", *Journal of Strategic Studies* (2021): pp. 1-36.

[42] Allan R. Millet and Williamson Murray, "Lessons of War", *The National Interest* Winter 1988/9, no. 14 (Winter 1988/9): pp. 83.

[43] For the purposes of this essay, the "national interest" is an abstraction, perhaps best defined as that which attempts to provide for one's own security or self-interest in the face of uncertain environmental conditions. This conception of the national interest opposes the notion that the national interest can be supplanted by or significantly altered by cyber. Here, cyber can be understood as a tool which serves the ends of security and self-interest; it is not an end itself.

other means."[44] The above analysis shows that the inclusion of cyber does not change the role of war as an instrument of policy, nor does it transform the fundamental drivers of politics and strategy. The goals of policy and strategy are more or less given to international actors, the most fundamental of which is possibly the nation-state's desire for survival in the face of environmental adversity and uncertainty. Since security and war are understood in terms of unchanging political and strategic drivers, it is, therefore, possible to incorporate and understand cyber using the old paradigms of security and war.

The thesis that cyber has fundamentally changed the nature of security and war is not so obvious given the debatable validity of its supporting arguments, which are that cyber is itself so important that it could be viewed as an end rather than a means, and that cyber creates unprecedented levels of instability. Neither of these arguments are conclusively true, which leaves room to explore how cyber might be explainable through existing, traditional theoretical tools. Accordingly, this essay has applied theories grounded in traditional security—such as information warfare, the offense-defense balance, and deterrence—to cyber. The essay has thus demonstrated that cyber can be understood through the language of traditional theories of international security and war, and in so doing, it has intimated that security and war have not been so altered by cyber that the study of cyber in international security precludes the use of existing theories.

The timeless and enduring drivers, goals, and purpose of security and war are exactly that — timeless and enduring. Technological sophistication in the form of cyber is ultimately superficial. Cyber may well change the form, means, and manner in which war "fighting" is conducted, but it will do little to change the fundamental purpose, which is the larger policy and strategic dimensions of security and war.

[44] Hugh Smith, *On Clausewitz: A Study of Military and Political Ideas*, (London: Palgrave Macmillan, 2004), pp. 98-99; Online Library of Liberty, "Clausewitz: War as Politics by Other Means", *Liberty Fund Network*, accessed October 5, 2021, https://oll.libertyfund.org/page/clausewitz-war-as-politics-by-other-means.