Oxford Research Encyclopedia of Politics

Power, Conflict, and Technology: Delineating Empirical Theories in a Changing World

Anthony J. S. Craig and Brandon Valeriano

Subject: World Politics Online Publication Date: Sep 2017 DOI: 10.1093/acrefore/9780190228637.013.587

Summary and Keywords

Technology has been given relatively scant attention in empirical international relations scholarship, despite its obvious importance to issues of military power and global security. Much progress is yet to be made into developing a fuller and more precise understanding of the interaction between technology and international relations. Synthesizing existing research will provide a clearer picture of the state of the field with regards to conceptualizing technology, the proliferation of technology, the technological component of national power, the impact of technology on international relations, the information and communication technology revolution and cyber security, and technology in international digital politics. This synthesis highlights key questions regarding what empirical research has to engage with and provides the first step toward addressing these issues.

Keywords: technology, power, diffusion, proliferation, innovation, cyber security, empirical international relations theory

Introduction

Technology holds a peculiar position in international relations scholarship. Despite its obvious importance to issues of military power and global security, it has received remarkably little systematic attention in the academic literature (Buzan & Herring, 1998, p. 8; Weiss, 2005, p. 296). According to Herrera (2007, p. 193), “existing theories of international relations treat technology as an afterthought or residual variable” rather than intertwined with politics. With the exception of offense–defense balance theory, which includes technology as one of a number of independent variables, there is little overarching theory or understanding of how technology spreads through the international system, its relationship to state power, or its consequences for international security. This is strange given the widespread acceptance that innovations in military technology can reshape the dynamics of the battlefield or even the international system.

The term “revolution in military affairs” is most commonly used to describe the technological advantage that states such as the United States held during the first Gulf War, which allowed for a rapid, decisive military victory with minimal casualties. History is, in fact, replete with examples of how technological breakthroughs impacted international politics. For example, much has been written about how the longbow allowed an outnumbered English army to defeat the French during the Hundred Years War, how tanks and airpower enabled Nazi

Germany's highly effective "Blitzkrieg" strategy, or how nuclear weapons technology created a powerful deterrent effect and increased stability between the United States and Soviet Union. Yet, there is no simple story about how technology alters battlefield outcomes. Horowitz (2010) documents the many challenges states face in achieving technological innovation including internal hindrances and financial limitations.

The importance of technology is as relevant today as it ever was. The revolution in information and communication technology (ICT) aided by the development of the internet has reshaped how states interact, how leaders appeal to their populations, and the structure of economic relationships. It has also led to the emergence of new national security threats as states become dependent on ICT and are vulnerable to acts of cyber-espionage, network disruptions, and the targeting of critical infrastructure by nonstate actors or rival governments.

This chapter brings together the often-disconnected empirical scholarship, that is, research based on observation and testable hypotheses, to evaluate the current state of the literature and to develop a more general understanding of the interaction between technology and international affairs. This chapter is structured as follows: after defining the concept of technology, it looks at the dynamics behind the proliferation of technology. Then, it investigates technology as a source of national power which has mostly been neglected in the literature. Fourth, this chapter reviews the arguments relating to the consequences of technology on international relations. Next, the focus moves to the area of cyber security, an issue that has arisen in international politics since the information revolution. Finally, the shift toward examining the latest studies on the impact of ICT technology on domestic politics and repression is outlined.

What is Technology?

The term technology is frequently used to describe two distinct concepts in military affairs. As Skolnikoff (1993, p. 13) notes, the confusion is "whether technology should be thought of as a piece of physical hardware" or as "the knowledge base that made the hardware possible." This is a very important distinction. When we talk of technology as hardware, or as Ross (1993) puts it: the "actual instruments or artefacts of warfare." This refers to the planes, ships, guns, and other products of a design and manufacturing process. In the age of cyber conflict, this definition can be expanded to include the software developed for cyber offense and defense. The second meaning of technology relates to the capacity of an actor to innovate and produce the technological hardware. This depends on economic size, industry, and organization, but there appears to be consensus in the literature that knowledge is key. For example, Weiss (2005) defines technology is "the practical application of technical knowledge." Technology is an important independent variable in lateral pressure theory (Choucri & North, 1989) of a state's territorial expansion, which they define in terms of knowledge and skills. Moreover, Skolnikoff (1993) distinguishes technology as hardware from "the knowledge, techniques, and procedures for carrying out tasks." Finally, Brooks (1980) views technology as the "knowledge of how to fulfil certain human purposes in a specifiable and reproducible way." As Herrera (2007, p. 4) points out, technology is a political problem, and our analysis of the factor requires understanding of the sociotechnical system. Applying this consideration to the international system elicits talk about states that possess a latent technological capacity in terms of knowledge base and that are considered in terms of possessing the technological hardware produced by this capability. The interaction between these two concepts is described by Buzan and Herring (1998), who view the ability of a state to independently produce advanced weapon systems as a key determinant of the distribution of military power, which can be redressed somewhat through the arms trade in the technological products themselves.

Technology, generally, is purely scientific in intent, but it is obviously caught up in the political process. Once this happens, generally benign technologies can have destructive military purposes. The question of dual-use technologies often drives debates about sanctions, trade, and legal processes, but this is a political process generally out of the hand of the producers of the technology in the first place. Yet, given the incentives of the leading technological powers to maintain a qualitative advantage, there always remains a gap between the "haves" and "have nots" of technological capacity. The next section explores the factors that shape the proliferation of technology as hardware which is often driven by a latent technological capability.

Causes of Technological Proliferation

Grand theories of international relations have painted a simplistic picture of technological diffusion by assuming that military technology is easily and rapidly reproduced throughout the international system. In Waltz's (1979) neorealist theory, "contending states imitate the military innovations contrived by the country of greatest capability and ingenuity. And so the weapons of major contenders, and even their strategies, begin to look much the same all over the world" (p. 127). Similarly, Gilpin (1981), argues that "although technology is expensive and not easily created, once it is created it usually diffuses relatively easily" (p. 177) from more advanced states to less advanced states. Offense–defense theory, moreover, effectively treats technology as a constant across countries because the theory's key independent variable is the prevailing nature of technology in the international system during a given historical period (Jervis, 1978; Van Evera, 1998).

The reality is, of course, more complex. According to Buzan and Herring (1998), the products of technological innovation spread throughout the international system in three ways. During the era of colonialism, arms could be transferred through the political and territorial expansion of the state, although this is rare today. Military technology will also spread as more states develop the manufacturing capacity themselves. The third and most common process of diffusion is that of the arms trade, whereby the few states with the technological and industrial capacity to produce weapon systems export their products to less capable states.

Horowitz (2010) focuses on the diffusion of military technology after a major innovation in military technology has occurred and introduces an "adoption-capacity" theory to explain how other states respond. The theory, supported through the cases of carrier warfare, nuclear weapons, battlefield warfare, and suicide terrorism, demonstrates how a combination of financial and organizational barriers determine whether states adopt the technology fully, adopt it partially, develop a different technology, move towards political neutrality, or form an alliance with the innovator.

The literature has since expanded beyond nuclear weapons to include space programs and capabilities (Early, 2014) and advanced and armed unmanned aerial vehicles (UAVs) (Horowitz & Furhmann, 2015). What these studies have in common is their use of an interest and capacity—also known willingness and opportunity (Most & Starr, 1989)—theoretical framework. Interest-based explanations see the adoption of a technology or related policy as a function of the state's motivations such as security concerns. Capacity-based explanations, on the other hand, view the process in terms of the ability of the state to develop or acquire it.

Interest

Interest-based factors, also known as willingness, or demand-side factors, are clearly important determinants of the acquisition of the products of technological innovation as demonstrated by the empirical literature. The most prominent interest-based explanation for a state acquiring a technology is external security threats. This is based in the neorealist view of the anarchical international system in which states view one another with suspicious and adopt policies to become more secure and ensure their survival. In line with this hypothesis, Singh and Way (2004) show that states with enduring rivals and frequent dispute engagement of are more likely to explore and acquire nuclear weapons. Using a different measure, Jo and Gartzke (2007) also show that conventional threat is positively and significantly associated with proliferation, although they also find that states with rivals with nuclear weapons are significantly less likely to acquire nuclear weapons.

Security-based explanations are also important in explaining the adoption of other, nonnuclear, technologies. The spread of UAVs, or drones, to greater numbers of states is an important topic because of their potential to revolutionize the conduct of warfare. Horowitz and Fuhrmann (2015, p. 5) find that states with a higher perception of terrorist threat is strongly linked to the acquisition of armed UAV's, and states with territorial disputes are more likely to acquire advanced drones, defined by their high durability and operating range, given their surveillance capabilities. Furthermore, Early (2014) finds that the more rivals a state has that possess domestic space launch capabilities, the more likely it is to develop similar capabilities.

Several scholars have posited a range of domestic factors that will affect its interest in acquiring technology. Sagan's (1996) domestic politics model for the spread of nuclear weapons suggests that interest groups within the state, including military bureaucracies, the nuclear energy industry, and politicians form coalitions to exploit national security concerns and influence government nuclear policy to promote their self-interests. Others debate the issue in terms of regime type, namely, that autocracies are less constrained by public opinion in pursuing nuclear weapons (Chubin, 1994; Sheikh, 1994; Kincade, 1995), or whether populist politicians within democracies are more likely to push for nuclear weapons development (Perkovich, 1999, pp. 404–424; Nizamani, 2000; Snyder, 2000). Empirical findings appear to support the latter argument (Jo & Gartzke, 2007, p. 179).

In drone proliferation, regime type also matters in that both the most democratic and autocratic countries are most likely to seek drones, albeit for different purposes (Horowitz & Furhmann, 2015). It remains unclear, however, whether the military industrial complex idea that Sagan (1996) proposed matters in technological proliferation.

Finally, there is the constructivist-based argument regarding nuclear proliferation. Sagan's (1996) norms model for the spread of nuclear weapons suggests that states may seek nuclear weapons as a status symbol or may abstain due to the spread of global norms of nonproliferation. Evidence from the nuclear literature is mixed (Jo & Gartzke, 2007). Using the novel measure of Olympic games performance, Early (2014) fails to find a relationship between prestige-seeking states and the development of space capabilities.

Capacity

A state can acquire an advanced weapons system either by possessing the technological capability to develop it, or it can acquire them from other states, such as via the arms trade. This ability of a state to develop or acquire technologies, also referred to as opportunity, or supply-side factors, will also determine what states acquire a capability and when. In the nuclear proliferation literature, the latent capacity to develop nuclear weapons, as measured by the possession of nuclear related materials and expertise, is positively associated with nuclear weapons development (Jo & Gartzke, 2007; Kroenig, 2010). For states lacking the independent production

capabilities, the transfer between states of designs, fissile material, and aid in the construction of facilities are also significant predictors of nuclear proliferation (Kroenig, 2010).

Findings by Early (2014) demonstrate in depth the importance of capacity-based explanations for predicting technological proliferation by looking at the acquisition of civil space agencies, satellite capabilities, and space-launch capabilities. Not only is economic size important but science and technological human capital are also critical factors in explaining developments in the space domain, as well experience in research and development in rocketry. The broader conclusion from this is the importance of separating technological expertise from economic capacity in explaining the spread of technologies to more states, as some studies fail to do. Horowitz and Fuhrmann (2014), for instance, use economic development (as measured with GDP per capita) as a proxy for technological sophistication. It is wrong to conflate these two concepts, however, because technological capacity involves non-economic factors such as knowledge.

In empirical research, the question of proliferation has been tackled from the perspective of specific weapons technologies and has been dominated by nuclear-related studies in particular. There is no development of theory to explain proliferation more generally. Therefore, research can continue in two ways. As has already begun, scholars should explore other significant products of technological processes, such as cyber capabilities.

Conversely, scholars may want to look at how states gain the technological production capabilities in the first place and why they are more likely to become technological leaders, rather than focus on specific technological products. Hyman's (2012) makes the critical point that developing countries sometimes make it difficult for the scientific process to take place because they impede the professionalism inherent in the field. More work needs to be done on the process of technological capability acquisition and how this process takes place in the digital arena.

Technology as a Component of National Power

Power is central in the study of international politics, particularly for realist international relations scholars who argue that the state must acquire material forms of power to become secure in an anarchical world. Power-related factors are also key variables in most realist explanations for war. For instance, the number of great powers in the international system (polarity), the distribution of power between states, and the transition of power between hegemons and challengers are some of the main factors affecting the likelihood of international conflict in structural realist theories.

Scholars adopting positivist methodologies have naturally set out to measure national power and test such theories. Power is a contentious term (Baldwin, 2013), but in these research programs it is often conceptualized in terms of material capabilities, referring to the set of resources and assets an actor possesses that increase its ability to achieve preferred outcomes such as winning wars. Surprisingly, however, technological capacity is rarely acknowledged as a component of national power, despite the qualitative military advantage that a more technologically advanced state is expected to hold. As Morgenthau (1948) writes, "the fate of nations and of civilizations has often been determined by a differential in the technology of warfare for which the inferior side was unable to compensate in other ways" (p. 136).

The most widely used measure, the Composite Index of National Material Capabilities (CINC) (Singer, 1987) may fail to fully account for the ability of a state to develop new technologies. The CINC was first developed to

examine the link between changes in the distribution of capabilities and the incidence of war in the international system (Singer, Bremer, & Stuckey, 1972). It has been used frequently as an independent or control variable since. The index measures the proportion of total system capabilities held by each state and captures the demographical, industrial, and military dimensions of power. The individual variables are total population, urban population, iron and steel production, energy consumption, military personnel, and military expenditure. Factors considered key in explaining a state's technological power, such as levels of expertise, knowledge, or skills are not directly captured by these variables, however. Given the CINCs widespread use in the field, the role of technology in shaping military capabilities is not being fully appreciated as a dimension of national power in many studies. Measuring levels of scientific or engineering education in a country, for instance, may provide a more accurate indicator of the state's ability to produce more sophisticated and effective weapon systems than its rivals. Assessing whether CINC is failing to account for technological capability is an obvious area for empirical research.

Furthermore, attempts to measure technological capability in the national power literature have often been flawed. First, some studies adopt an ungeneralizable measure that is only relevant for the particular weapons system they seek to explain. For example, Meyer (1984) develops a set of latent nuclear technological capacity indicators that have been used in updated forms to explain nuclear weapons proliferation (Stoll, 1996; Jo & Gartzke, 2007). The variables include national mining activity, indigenous uranium deposits, metallurgists, steel production, construction workforce, chemical engineers, nitric acid production, electric production capacity, nuclear engineers, physicists, and chemists, and explosives and electronics specialists. Clearly, these would be unsuitable in explaining the adoption of other weapons systems or innovations and cannot offer an overall estimation of levels of technological advancement in a country.

The second issue is that some scholars use measures that are so broad that they may fail to capture the concept they intend to. In some studies (Singh & Way, 2004; Horowitz & Furhmann, 2014), scholars use GDP per capita as a proxy for technological capacity. Although these two variables are likely correlated, GDP per capita is a more accurate measure of economic development, which is a distinct concept from technological capacity. There is clearly more to technology than economic factors. This distinction is demonstrated by Early (2014) in explaining the proliferation of space capabilities. He measures a country's science and technology human capital using data on higher education graduates while controlling for economic factors separately. Both variables are shown to have independent effects on the dependent variables. Education may be a crucial ingredient of technological capacity, yet one that GDP-related variables may fail to gauge precisely.

The lack of methodological consistency between studies signifies a lack of engagement with the question of what technological power really means and a failure to make empirical progress. The challenge for scholars, therefore, is to create an improved measure of a state's general technological capacity that both precisely captures the concept they seek to measure and is also applicable across a broad range of research questions. If technological capability refers to the resources and assets a state possesses increasing its ability to make scientific advances, then factors including scientific education, knowledge, or expertise appear to be crucial considerations.

Consequences of Technology for International Relations

Perhaps the closest the field has come to articulating a theory to account for the effect of technology is that of the offense–defense balance. The theory is used to explain the likelihood of war, and other destabilizing phenomena such as arms races, based on the relative appeal of conquering territory over defending territory. As one of the

originators of the theory, Jervis (1978, p. 187), explains: “When we say the offense has the advantage, we simply mean that it is easier to destroy the other’s army and take its territory than it is to defend one’s own. When the defense has the advantage, it is easier to protect and to hold than it is to move forward, destroy, and take.”

Technology plays a central role in the theory as one of the main determinants of the offense–defense balance. Although many scholars use a broader set of factors including geography (Jervis, 1978), military doctrine (Van Evera, 1998), or force employment (Biddle, 2005), the “core” version of the theory focuses purely on the nature of military technology (Lieber, 2005, p. 29). Countless arguments have been put forward to explain the effect of specific innovations on the balance, yet the most frequently cited in the literature concern mobility-enhancing and firepower-enhancing technologies. Firepower-enhancing technologies are said to favor the defense because they render an advancing attacking force more vulnerable to fire from defenders in protected positions. Mobility enhancing technologies, on the other hand, are said to favor the offense because they allow for the outflanking of defenders or for the concentration of forces to exploit the defense’s weak spots (Glaser & Kaufmann, 1998, p. 7).

The theory relies on the technological determinist argument that, throughout history, technology has explained the onset or absence of war. For instance, prior to WWI, the revolution in small arms and artillery created a widespread, albeit mistaken, belief among European leaders in the “cult of the offensive” that encouraged them to launch pre-emptive wars or risk being attacked themselves. In reality, technology heavily favored the defense, as the stalemates of trench warfare demonstrate. World War II has been explained in terms of the offensive advantage created by mobility enhancing motorized vehicles, especially the tank, which enabled and encouraged Germany’s blitzkrieg strategy. Furthermore, it is argued that the enormous increase in firepower potential arising from the invention of nuclear weapons shifted the balance heavily in favor of the defense and prevented U.S.–Soviet conflict during the Cold War (Van Evera, 1998). Yet, the issue is complicated and technology is likely but one factor of many that explains the absence of war during the Cold War (Vasquez, 1991).

Offense–defense balance has come under intense criticism for, among other things, the categorization of certain technologies as either offensive or defensive, its immeasurability, and its lack of parsimony (Davis, Finel, & Goddard, 1998). The decision to go to war is not based on technological factors, as Mearsheimer (1983) argues, but by the prospects for a quick victory. Similarly, Lieber (2005) claims that political considerations trump technological conditions in explaining war. Most problematic perhaps is that many scholars treat technology as a system-level variable (Lynn-Jones, 1995), assuming that technology has diffused completely to all states, which is not necessarily true.

The empirical support is, moreover, very limited. By coding historical eras into offense, defense, or deterrence dominant, Adams (2003) measures the effects of the offense–defense balance on the incidence of attacks and conquest and finds support for the theory. In a separate study, on the other hand, Gortzak et al. (2005) find no link between either the perceived or actual offense–defense balance and the incidence of militarized interstate disputes and war. The divergent findings can probably be put down to the different methodologies employed between the two studies, as seen in the choice of dependent variables, or in the coding procedures for historical time periods. More tellingly, Adams fails to include a number of control variables unlike Gortzak et al. who, as a result, find that other variables, such as regime type, better explain the incidence of interstate conflict.

Given the theoretical and empirical weaknesses, scholars are wise to move beyond this structural theory of technology. Biddle (2005) looks at the issue at the dyadic level but finds that technology (as measured by superior weapons systems), or other forms of capability for that matter, has very little bearing on military victory. Instead, he proposes a theory that force employment is a more powerful explanation of military outcomes, which he

supports with extensive statistical testing. As Tang (2010) suggests, a way forward would be to use a measure of "technological sophistication" of the state to test the impact of technology, although his suggestion of using GDP per capita for this purpose is flawed. What is needed is a new measure of technological capacity as an independent variable to investigate our research questions.

Cyber Security and International Relations

The most recent technological shift has been the digital, or cyber, revolution. A host of new cyber threats have emerged from the development of the Internet and the vulnerability it places on governments and society (Dunn Cavelty, 2007). The problem of research in this area, however, is that many claims are made about the impact of cyber technologies on international security that are not supported by empirical evidence. Despite a widespread belief that data are difficult to collect in this domain (Kello, 2013), there is in fact, progress has been made in this area (Valeriano & Maness, 2015), and there is still much opportunity for scholars to collect quantitative data and design case studies to develop empirical theories relating to the cyber domain.

One of the claims made about cyberspace is that because offensive cyber capabilities are cheaper and easier to develop, as well as more instantaneous, attacking is a more effective strategy; thus, we will see an escalation in cyber warfare (Lieber, 2014, pp. 100–103). Offensive capabilities are considered more cost-effective in that "another dollar's worth of offense requires far more than another dollar's worth of defense to restore prior levels of security" (Libicki, 2009, p. 32).

Yet, even if developing malware is cheaper than constructing effective defenses, a point unproved, it is not necessarily true that offensive operations will be effective. Even the most sophisticated of attacks such as Stuxnet, were highly limited in their impact against the designated target (Lindsay, 2013). There is little evidence that coercion is really possible cyberspace, especially as a domain-specific tactic (Jensen, Maness, & Valeriano, 2017).

While there is evidence of an increasing trend toward the use of cyber as a means to engage in conflict (Valeriano & Maness, 2014, 2015), there is a general evident level of restraint in this domain given that states have refrained from escalation (Valeriano & Maness, 2015) and outright violence (Rid, 2013). Restraint is observed because of the nature of the weapons prevents disclosure due to the possibility of reuse, the high probability impacts on civilians, the establishment of norms, and the risk involved in attempting actions that have never been undertaken before.

A related notion is that given their low cost, the tools of cyber warfare confer advantages to conventionally weaker states and can reconfigure the traditional structure of the international system (Lango, 2016, p. 12; Nye, 2011). Traditional power dynamics may also be challenged by the increased dependency that the most technologically advanced countries are on ICT which renders them more vulnerable to a crippling cyber-attack than less developed nations (Kolet, 2001, p. 282). Gartzke (2013) challenges this idea on theoretical grounds, writing that "It is one thing for an opponent to idle a country's infrastructure, communications or military capabilities. It is quite another to ensure that the damage inflicted translates into a lasting shift in the balance of national capabilities or resolve" (p. 2). It may be that cyber technology only contributes to military effectiveness when used in conjunction with conventional military operations.

Empirical evidence, moreover, generally suggests that strong states seek to challenge weaker powers in cyberspace (Valeriano & Maness, 2015). While some weaker states like North Korea seek to expand their influence through cyber means, this is not at all out of character for an ambitious, revisionist state. More often than not, the small state is the target rather than the initiator, and this is a key distinction for cyber power relationships. In fact, there is a strong correlation between nuclear power and cyber conflict (Pytlak & Mitchell, 2016), suggesting that cyber means really seems to embolden and aid strong states.

The issue of coercion then comes to the forefront. Can cyber means be used to compel the target to either concede short of war or during war? Evidence finds that this situation is rare in cyber affairs, of a 192 cases of compellent action in cyberspace, only 12 have resulted in a change in behavior for the target (Jensen, Maness, & Valeriano, 2017). The story of these 12 cases paints a complicated picture where the resulting change in behavior was not exactly what was intended. For example, the North Koreans were successful in compelling action when they hacked Sony in 2014, but the movie they sought to prevent from being released was in fact given away for free, expanding its visibility internationally. What states get in cyberspace is not exactly what they aim to achieve.

Furthermore, Kostyuk and Zhukov (2015) present novel evidence that Russia has not been achieving battlefield effects with cyber tactics in Ukraine. Certainly, more studies are needed that examine the means of change through cyber power, but the preliminary results challenge the idea that cyber technologies are effective means of coercion, that these methods expand harm, and result in escalation.

The question remains whether digital technology increases the impulses for action in states regardless of evident restraint overall. Utilizing lateral pressure theory (Choucri, 2012, p. 29) argues that the individual level of action becomes more important in cyberspace as *Homo politicus* is “able to express both view and voice through cyber venues.” This new access through digital avenues would lead to aggregation of demands, fueling the expansionist or violent instincts of a state. Does technology really motivate action and drive aggression? This question is examined next in terms of the expansion of violence and demands for democracy through technological means.

Technology and International Digital Politics

Digital politics as a field of inquiry suggests that there is a new driver of interactions and international affairs, technology, and knowledge. As Choucri notes, “Cyberspace empowers and enables individuals in ways that were previously not possible. This empowerment is manifested through communication, expressed perceptions, organization, and preparations for action” (2012, p. 14). Others have extended the frame to the promotion of democracy and freedom, noting that the Internet and digital communication tools would be a positive force for change in the international system. In some ways, this theory has become known as the liberation technology thesis, succinctly advanced by Diamond (2010). The idea is that new communications technologies, including the Internet, mobile phones, and social media platforms, allow protestors and democracy advocates to better organize to advance their agendas.

Empirical research, in contrast, presents a more complicated picture. Information and communication technologies can negatively impact progress and freedoms due to the expansion of the power of government, particularly authoritarian governments, but they can also enable democracies already established (Milner, 2006). However, Rød and Weidmann (2015) advance a repression technology perspective finding that the Internet has not contributed toward the advancement of a new wave of democracy. Instead, “the result directly contradicts the

'liberation technology' argument, because one would expect such regimes [authoritarian] would be deterred from implementing a technology that enable free information to flow" (Rød & Weidmann, 2015). Research by King, Pan, and Roberts (2013) supports this view. To determine the level of control the Chinese government maintains over social media, they established their own social media network; the flow of information remains uncensored unless it leads to collective action and protests. A follow-up project by the same group (King, Pan, & Roberts, 2017) reports that the millions of posts the Chinese government creates are meant to distract or direct the public to following certain narratives, while minimizing other ideas.

Turning directly to conflict and away from protests and democracy, a complicated picture regarding ICTs and peace emerges. The empirical results suggest a dangerous combination of digital technology and violence; for example, Warren (2015) demonstrates a linkage between cellular access and collective violence. At the same time, access to traditional media, as measured by radio connections, decreases violence. Bailard's (2015) results indicate that access to mobile technologies can increase the probability of armed conflict between insurgents and government, thus lending support to Warren's (2015) model and empirical findings.

Gohdes (2015) notes a correlation between repression and pulling the plug on digital technology. States would have an incentive to limit access to digital communication devices during times of protest and organization; thus, there is a high likelihood that states will marshal the power to limit digital communications. Rather than being an enabler, the state can use its control over communications to limit organization and maintain its control over the population. States can also use digital technology to reduce insurgent violence by providing for avenues of information flows to counter aggressive combat forces present in Iraq during the long war (Shapiro & Weidmann, 2015). More empirical evidence is needed on the limiting influence of technology on advancement; in fact, it may be an enabling factor of both violence and a source of state-based repression. This line of research needs to engage evidence as more incidents and events accumulate challenging the most positive predictions of technology aiding the process of peace.

Conclusion

Many scholars in the field of technology, innovation, and national security see a clear progression between technology and the advancement of power projection capabilities. The problem is that this idea is a bit too simple for the complexity inherent in technological advancement. There is no direct causal link between technology and the drivers of changes in the international system; instead, the casual chain is convoluted, complex, and delayed in many cases. This empirical complexity needs to be reflected in the research and scholarship; instead, it is dominated by hyperbolic statements about rapid changes brought on by technology. Some pessimism about the rapid changes brought about by technology is necessary to advance a more nuanced and accurate representation of the changes brought on by the digital technology.

Current research presents a rather mixed set of findings regarding technology and conflict. The main takeaway is that scholars need to advance an empirical perspective when they engage innovation and technology. Dramatic changes have been brought on by technology, but in reality, this process has always been a complicated one that can take generations, promotes regressions and repression, and sometimes enables major powers to maintain a monopoly on violence. Digital technology has promoted change, but this change is complex and nuanced.

References

Adams, K. R. (2003). Attack and conquer? International anarchy and the offense-defense-deterrence balance. *International Security*, *28*(3), 45–83.

Find this resource:

Bailard, C. S. (2015). Ethnic conflict goes mobile: Mobile technology's effect on the opportunities and motivations for violent collective action. *Journal of Peace Research*, *52*(3), 323–337.

Find this resource:

Baldwin, D. A. (2013). Power and international relations. In W. Calrsnaes, T. Risse, & B. A. Simmons (Eds.), *Handbook of International Relations* (pp. 273–297). London: SAGE.

Find this resource:

Biddle, S. (2005). *Military power: Explaining victory and defeat in modern battle*. Princeton, NJ: Princeton University Press.

Find this resource:

Brooks, H. (1980). Technology, evolution, and purpose. in modern technology: Problem or opportunity? *Daedalus*, *109*(1), 65–81.

Find this resource:

Buzan, B., & Herring, E. (1998). *The arms dynamic in world politics*. London: Lynne Reinner.

Find this resource:

Choucri, N. (2012). *Cyberpolitics in international relations*. Cambridge, MA: MIT Press.

Find this resource:

Choucri, N., & North, R. C. (1989). Lateral pressure in international relations: Concept and theory. In M. I. Midlarsky (Ed.), *Handbook of war studies*. Ann Arbor: University of Michigan Press.

Find this resource:

Chubin, S. (1994). The Middle East. In M. Reiss & R. S. Litwak (Eds.), *Nuclear proliferation after the Cold War* (pp. 33–66). Cambridge, MA: Ballinger.

Find this resource:

Davis, J. W., Finel, B. I., & Goddard, S. E. (1998). Correspondence: taking offense at offense defense theory. *International Security*, *23*(3), 179–206.

Find this resource:

Diamond, L. (2010). Liberation technology. *Journal of Democracy*, *21*(3), 69–83.

Find this resource:

Dunn Cavelty, M. (2007). *Cyber-security and threat politics: US efforts to secure the information age*. Routledge.

Find this resource:

Early, B. R. (2013). Exploring the final frontier: An empirical analysis of global civil space proliferation. *International Studies Quarterly*, *58*(1), 55–67.

Find this resource:

Early, B. R. (2014). Exploring the final frontier: An empirical analysis of global civil space proliferation. *International Studies Quarterly*, *58*(1), 55–67.

Find this resource:

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR) Relevant theory? *International Political Science Review*, *27*(3), 221–244.

Find this resource:

Fuhrmann, M., & Horowitz, M. C. (2014). When leaders matter: rebel experience and nuclear proliferation. *Journal of Politics*, *77*(1), 72–87.

Find this resource:

Gartzke, E. (2013). The myth of cyberwar: Bringing war on the internet back down to earth. *International Security*, *38*(2), 41–73.

Find this resource:

Gartzke, E., & Jo, D.-J. (2007). Determinants of nuclear weapons proliferation. *Journal of Conflict Resolution*, *51*(1), 167–194.

Find this resource:

Gilpin, R. (1981). *War and change in world politics*. Cambridge, U.K.: Cambridge University Press.

Find this resource:

Glaser, C. L., & Kaufmann, C. (1998). What is the offense-defense balance and can we measure it? *International Security*, *22*(4), 44–82.

Find this resource:

Gohdes, A. R. (2015). Pulling the plug: Network disruptions and violence in civil conflict. *Journal of Peace Research*, *52*(3), 352–367.

Find this resource:

Gortzak, Y., Haftel, Y. Z., & Sweeney, K. (2005). Offense-defense theory: An empirical assessment. *Journal of Conflict Resolution*, *49*(1), 67–89.

Find this resource:

Herrera, G. L. (2007). *Technology and international transformation: The railroad, the atom bomb, and the politics of technological change*. New York: SUNY Press.

Find this resource:

Horowitz, M. C. (2010). *The diffusion of military power: Causes and consequences for international politics*. Princeton, NJ: Princeton University Press.

Find this resource:

Horowitz, M. C. & Fuhrmann, M. (2015). **Droning on: Explaining the proliferation of unmanned aerial vehicles**. *Social Science Research Network*.

Find this resource:

Hymans, J. E. C. (2012). *Achieving nuclear ambitions: scientists, politicians, and proliferation*. Cambridge, U.K.: Cambridge University Press.

Find this resource:

Jensen, B., Maness, R. C., & Valeriano, B. (2017). Cyber compellence: The efficacy of cyber power. Unpublished manuscript.

Find this resource:

Jervis, R. (1978). Cooperation under the security dilemma. *World Politics*, *30*(2), 167–214.

Find this resource:

Kello, L. (2013). The meaning of the cyber revolution hypothesis. *International Security*, *38*(2), 7–40.

Find this resource:

Kincade, W. H. (1995). *Nuclear proliferation: Diminishing threat? INSS Occasional Paper 6*. U.S. Air Force Academy: USAF Institute for National Security Studies, Colorado Springs.

Find this resource:

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review*, *2*(107), 1–18.

Find this resource:

King, G., Pan, J., & Roberts, M. E. (2017). How the Chinese government fabricates social media posts for strategic distraction, not engaged argument. *American Political Science Review*, *111*(3), 484–501.

Find this resource:

Kolet, K. S. (2001). Asymmetric threats to the United States. *Comparative Strategy*, *20*(3), 277–292.

Find this resource:

Kostyuk, N., & Zhukov, Y. (2015). Invisible digital front: The Logic of cyber and kinetic operations in Ukraine. Peace Science Society Annual Meeting, Oxford, Mississippi.

Find this resource:

Kroenig, M. (2010). *Exporting the bomb: Technology transfer and the spread of nuclear weapons*. Ithaca, NY: Cornell University Press.

Find this resource:

Lango, H.-I. (2016). Competing academic approaches to cyber security. In K. Friis & J. Ringsmose (Eds.), *Conflict in cyber space: Theoretical, strategic and legal perspectives*. London: Routledge.

Find this resource:

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, CA: Rand.

Find this resource:

Lieber, K. (2014). **The offense-defense balance and cyber warfare**. In E. O. Goldman & J. Arquilla (Eds.), *Cyber analogies*. Monterey, CA: Naval Postgraduate School.

Find this resource:

Lieber, K. A. (2005). *War and the engineers: The primacy of politics over technology*. Ithaca, NY: Cornell University Press.
Find this resource:

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365–404.
Find this resource:

Lynn-Jones, S. M. (1995). Offense-defense theory and its critics. *Security Studies*, *4*(4), 660–691.
Find this resource:

Mearsheimer, J. J. (1983). *Conventional deterrence*. Ithaca, NY: Cornell University Press.
Find this resource:

Meyer, S. M. (1984). *The dynamics of nuclear proliferation*. Chicago: University of Chicago Press.
Find this resource:

Milner, H. V. (2006). The digital divide: The role of political institutions in technology diffusion. *Comparative Political Studies*, *39*(2), 176–199.
Find this resource:

Morganthau, H. J. (1948). *Politics among nations: The struggle for power and peace*. New York: Alfred A. Knopf.
Find this resource:

Most, B. A., & Starr, H. (1989). *Inquiry, logic and international politics*. Columbia: University of South Carolina Press.
Find this resource:

Nizamani, H. K. (2000). *The roots of rhetoric: Politics of nuclear weapons in India and Pakistan*. Westport, CT: Praeger.
Find this resource:

Nye, J. S. (2011). *The future of power*. New York: Public Affairs.
Find this resource:

Perkovich, G. (1999). *India's nuclear bomb: The impact of global proliferation*. Berkeley: University of California Press.
Find this resource:

Pytlak, A. & Mitchell, G. E. (2016). Power, rivalry and cyber conflict: An empirical analysis. In J. Ringsmore & K. Friis (Eds.), *Conflict in cyber space: theoretical, strategic, and legal perspectives*. London: Routledge.
Find this resource:

Rid, T. (2013). *Cyber war will not take place*. London: C. Hurst.
Find this resource:

Rød, E. G., & Weidmann, N. B. (2015). Empowering activists or autocrats? The Internet in authoritarian regimes. *Journal of Peace Research*, *52*(3), 338–351.
Find this resource:

Ross, A. L. (1993). The dynamics of military technology. In D. Deitt, D. Haglund, & J. Kirton (Eds.), *Building a new global order: Emerging trends in international security*. Oxford: Oxford University Press.
Find this resource:

Tang, S. (2010). Offense-defence theory: Towards a definitive understanding. *The Chinese Journal of International Politics*, *3*(2), 213–260.
Find this resource:

Sagan, S. D. (1996). Why do states build nuclear weapons? Three models in search of a bomb. *International Security*, *21*(3), 54–86.
Find this resource:

Shapiro, J. N., & Weidmann, N. (2015). Is the phone mightier than the sword? Cell phones and insurgent violence in Iraq. *International Organization*, *69*(2), 247–274.
Find this resource:

Sheikh, A. T. (1994). Pakistan. In M. Reiss & R. S. Litwak (Eds.), *Nuclear proliferation after the Cold War* (pp. 191–206). Cambridge, MA: Ballinger.
Find this resource:

Singer, J. D. (1987). Reconstructing the Correlates of War dataset on material capabilities of states, 1816–1985. *International Interactions*, *14*, 115–132.
Find this resource:

Singer, J. D., Bremer, S., & Stuckey, J. (1972). Capability distribution, uncertainty, and major power war, 1820–1965. In B. Russett (Eds.), *Peace, war, and numbers*. Beverly Hills, CA: SAGE.
Find this resource:

Singh, S. & Way, C. R. (2004). The correlates of nuclear proliferation: A quantitative test. *Journal of Conflict Resolution*, *48*(6), 859–885.
Find this resource:

Skolnikoff, E. B. (1993). *The elusive transformation: Science, technology, and the evolution of international politics*. Princeton, NJ: Princeton University Press.
Find this resource:

Snyder, J. L. (2000). *From voting to violence: Democratization and nationalist conflict*. New York: Norton.
Find this resource:

Stoll, J. R. (1996). **World production of latent nuclear capacity**.

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research*, *51*(3), 347–360.
Find this resource:

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. New York: Oxford University Press.
Find this resource:

Van Evera, S. (1998). Offense, defense, and the causes of war. *International Security*, *22*(4), 5–43.
Find this resource:

Vasquez, John. (1991). The deterrence myth: Nuclear weapons and the prevention of nuclear war. *The long postwar peace: Contending explanations and projections*, 205–223.
Find this resource:

Waltz, K. (1979). *Theory of international politics*. Reading, PA: Addison-Wesley.
Find this resource:

Warren, T. C. (2015). Explosive connections? Mass media, social media, and the geography of collective violence in African states. *Journal of Peace Research*, *52*(3), 297–311.
Find this resource:

Weiss, C. (2005). Science, technology and international relations. *Technology in Society*, *27*, 295–313.
Find this resource:

Anthony J. S. Craig

Research School on Peace and Conflict, Cardiff University

Brandon Valeriano

School of Law and Politics, Cardiff University