ANNUAL REVIEWS

Annual Review of Political Science

Do Emerging Military Technologies Matter for International Politics?

Michael C. Horowitz

Political Science Department, University of Pennsylvania, Philadelphia, Pennsylvania 19104-6215, USA; email: horom@sas.upenn.edu

Annu. Rev. Political Sci. 2020. 23:385–400

The *Annual Review of Political Science* is online at polisci.annualreviews.org

https://doi.org/10.1146/annurev-polisci-050718-032725

Keywords

weapons, technology, innovation, artificial intelligence, cyber, robotics, drones

Abstract

We live in a digital world. This fact has significant consequences for warfare. Two technologies in particular, cyber and drones, feature in military and intelligence operations and in scholarship. In addition, a new vein of scholarship is examining how advances in artificial intelligence have the potential to shape the future of warfare. While scholars disagree about the consequences of these technologies for international politics, they tend to agree that their consequences are mediated by the ability of military organizations, whether state or nonstate actors, to use them effectively in relevant military scenarios and in the pursuit of political ends. Studying newer military technologies, with less empirical evidence than is available for technologies that have been around for decades, also generates methodological challenges for research.

INTRODUCTION

The Information Age plays a growing role in politics. Political scientists both use digital tools and study how these tools matter for politics at home and abroad. That we live in a digital world matters for every sector of politics, from polling and survey data to how social media might both enable new forms of organized protest and help governments track and crack down on dissidents. The digital world has arguably had significant consequences for international politics and warfare as well. Although whether the "new" weapons of the twenty-first century are really new is contested, the use of digital technologies by militaries has grown—and scholarship on these technologies has grown as well. Cyber and drones are of particular interest as they play an increasing role in how countries and nonstate actors fight. In addition, a new vein of scholarship is examining how advances in artificial intelligence have the potential to shape the future of warfare.

This scholarship sometimes overlooks other technological changes that could impact global politics, such as synthetic biology and additive manufacturing, and its exploration of the drone and cyber phenomena has been limited in depth. Because these are newer military technologies, relatively little empirical evidence is available, and this paucity generates methodological challenges for scholarship. While scholars disagree about the consequences of these technologies for international politics, they tend to agree that their effects are mediated by the ability of military organizations to use them effectively in relevant battlefields and in the pursuit of political ends.

HOW DO WEAPONS SYSTEMS INFLUENCE INTERNATIONAL POLITICS?

If military power is how states use organized violence on battlefields, whether conventional or unconventional, weapons systems are tools that states employ in the pursuit of military power. Research on military systems and military power overwhelmingly suggests that, in general, what matters most for victory and defeat in warfare is how countries and nonstate actors use these tools (Biddle 2004, Horowitz 2010). Nuclear weapons, to most scholars, represent an exception—the rare case where the technology itself is thought to have significant consequences for international politics, almost aside from how countries might plan to use it (Jervis 1989). For most weapons, though, questions of strategies of usage, doctrine, force employment, organizational politics, and related issues are very important. Put another way, in social science work on technology and international politics, technology is either the dependent variable or a key independent variable. In explanations of the spread or use of technology, the drivers of proliferation in classic international relations arguments (security concerns, domestic politics, status seeking, etc.) become the key independent variables. Alternatively, scholars can use technology as a key independent variable to explain dependent variables such as deterrence success, the outbreak or escalation of war, crisis bargaining, and the like. The most successful work tends to connect to more traditional literatures in international relations, avoiding a balkanization of technology as a separate topic.

Studying new military technologies comes with challenges due to the limited available evidence, however. When the key usage cases for a military capability are ongoing, especially when it is a sensitive technology, getting access to enough information to draw inferences is difficult. This makes it hard to study technology and military effectiveness in some cases. For example, most research on military robotics focuses on drones, even though drones are only one of many ways that militaries or militant groups might employ military robotics. The reasons for the emphasis on drones include their public prominence and the accessibility of data on their usage in some cases (though there are still limits that influence scholarship on drones, as described below). A second challenge to scholarship is real world uncertainty surrounding an emerging technology that is influencing how militaries fight.

Scholars interested in studying emerging technologies such as new weapons systems do have research design options. One popular approach to studying new weapons technologies involves behavioral research on what influences attitudes toward them within the general public (Horowitz 2016, Kreps 2014, Walsh & Schulzke 2018), in the military, or among elites (Schneider 2019a). This approach circumvents the lack of historical evidence by framing research questions in terms of attitudes; questions might explore the willingness to use a particular technology on the battlefield in a given scenario, for example, or interest in adopting it for potential usage.

Another approach tailors research to ask questions that can be answered despite the limitations on data. One example, discussed below, involves work on drone strike campaigns in locations where evidence is available, such as Afghanistan. Another example is leveraging event data to study attempts to use technologies such as cyber for coercive purposes (Kostyuk & Zhukov 2019).

A third approach to studying emerging technologies is applied theory. In the study of new weapons systems, applied theory entails leveraging insights from existing international relations theory—or other fields—and applying them to limited existing evidence to assess how particular weapons systems are likely to shape international politics (Horowitz 2018, Rid 2013).

A fourth methodological option when empirical evidence is limited involves game theoretic models. Scholars use formal models to derive predictions about how new weapons will shape politics and then do limited case studies based on what evidence is available.

This article focuses for the most part on the two technologies that have generated significant interest on the part of international relations scholars over the last several years—drones and cyber. It also discusses the growth in research on how advances in artificial intelligence could shape international politics. Various other technologies also deserve attention, including but not limited to hypersonics, synthetic biology, and additive manufacturing. As these technologies have not been the subject of as much scholarship from international relations scholars (for some exceptions, see Koblentz 2011, Volpe 2019, Williams 2019), examining them is a task for a future review.

While this article approaches the topic of emerging military technologies and international politics by using the technology as the unit of analysis, that is certainly not the only possible angle. Another approach is to focus on the intersection of technology with classic questions for international politics, such as the potential for war (Fearon 2018), the risk of escalation (Talmadge 2019), the potential for arms races, or other topics (Sechser et al. 2019). A third way is to focus on particular facets of technologies, such as their potential to be disruptive in particular sectors, their complexity (Gilli & Gilli 2019), or whether they are dual use (Drezner 2019). As referenced above, it is critical to connect research on technology with broader research on international relations.

DRONES

Drone Strikes

Arguably, no emerging weapons technology has received more attention from scholars over the last decade than drones, because drones represent the most visible application of the Information Age to contemporary warfare. Drones are piloted remotely and have launch and landing capabilities. Unlike missiles, they are designed for repeated use (Horowitz et al. 2016). Note that it is possible to add a payload and use a drone as a one-way missile, as the attacks on Saudi oil facilities in September 2019 demonstrated. Drones are also sometimes called unmanned aircraft, uninhabited aircraft, or remotely piloted aircraft.[1] Debates in the literature surround the relative effectiveness of drone strikes, specifically the use of drones for counterterrorism and counterinsurgency

[1]In general, the preference should be to call them drones, uninhabited aircraft, or remotely piloted aircraft because those terms are not gendered.

operations generally by the United States. Research on drone strikes includes qualitative case studies surrounding US drone strike campaigns in Afghanistan, Pakistan, or elsewhere, as well as quantitative, micro-level data on the same campaigns. Scholars are divided about the effectiveness of drone strikes.

Those who conclude that drones are effective in counterterrorism and counterinsurgency argue that they are more efficient and cost-effective in accurately targeting adversaries than alternative uses of force such as inhabited aircraft or teams of soldiers on the ground (Byman 2013). The ability of drones to loiter for long periods of time over a target means that the attacker can gain better intelligence on the target and surrounding area, making a more accurate strike more likely. This reduces the risk of civilian casualties. From a purely military perspective, drone strikes may also decrease the capacity of militant groups to conduct subsequent attacks (Mir 2018). Johnston & Sarbahi (2016) use data on US drone strikes in Pakistan between 2007 and 2011 to show that drones reduce the risk of subsequent terrorist attacks, as well as the targeting of tribal elders by militant groups. There is also evidence that drone strikes do not broadly cause blowback by generating more militant group recruitment (Shah 2018).

An alternative line of argument suggests that drones are ineffective and lead to blowback that degrades the effectiveness of counterterrorism and counterinsurgency operations in many cases. Critics argue that drone strikes are often based on faulty intelligence and that the intelligence information that is most likely to lead to successful strikes comes from sources on the ground, meaning that even when attacks succeed, drones do not deserve the credit (Boyle 2013, Cronin 2013). Smith & Walsh (2013) find that drone strikes against al Qaeda did not, at least initially, significantly reduce al Qaeda's ability to generate propaganda. Critics also argue that the public in attacked locations tend to blame the attackers, not militant groups, meaning that attacks generate radicalization in the local population that makes further militant activity more likely and reduces the potential for local governments to cooperate with the attackers (Boyle 2013, Cronin 2013, Kilcullen & Exum 2009). Drone strikes can also generate international backlash due to the perception that strikes outside the context of recognized war zones are questionable under international law, leading to reputational costs.

The latter objection relates to the debate about decapitation strikes against terrorist groups. Drones are not the only military tool used for decapitation strikes, but, especially in areas that lack effective air defenses, drones are a popular tool for attacks designed to kill the leaders of insurgent and terrorist groups. Jordan (2009, 2014) argues that these attempts often fail and do not generally degrade group capabilities, but others disagree (Johnston 2012).

More recent work attempts to navigate these debates by studying, at an even more micro level, how drone strikes shape militant group behavior. Mir & Moore (2019), evaluating geocoded violence data and US–Pakistan counterterrorism cooperation, show that drones strikes succeeded at suppressing militant behavior, but often through anticipatory effects. Militant groups stopped communicating and planning attacks in an attempt to avoid being monitored and targeted.

There are methodological challenges associated with scholarship on drone strikes that reflect limits on data availability, among other issues. Whether drone strikes are considered effective depends on a range of research design decisions, including whether the dependent variable is a specific militant group or militant attacks in an area, the timeframe under evaluation, and the ability to incorporate the counterfactual costs of other types of strikes into the study. For example, drones might succeed in reducing the capability of a militant group in the short and medium term but also lead to public blowback that generates more radicalization over time. It is also possible that drones are more successful than inhabited aircraft or ground teams at reducing civilian casualties but that drone strikes still do lead to civilian casualties, and even significant civilian casualties at times. It is important for future research to incorporate military requirements into the evaluation

of the success of drone strikes. Some drone strikes occur because drones are the only asset in a given region with an appropriate type of munition for an attack. In other cases, those ordering a strike might have the ability to choose between different strike options. The counterfactual—what would happen if a drone strike did not take place—might matter a great deal when we attempt to answer questions concerning the impact of drone strikes.

The debate about drone strikes is by far the most developed subsection of the broader literature on technology and international conflict over the last few decades, and as such it features clearer debates, which help point the way toward opportunities for future research. There has been other research on drones, though the debates within the areas described below have not been as developed.

Public Attitudes Toward Drones

Some research evaluates public attitudes about drones, generally in the context of drone strikes. There is limited debate between scholars in this context. Drone strikes tend to be popular with the American public due to fear of casualties, with support crossing party lines between Democrats and Republicans (Walsh & Schulzke 2018). Scholars have investigated what explains this support and what could lead to variation. Soft support for drone strikes likely exists because drones are perceived as a way to strike at adversaries without putting US troops at risk (Kreps 2014, Walsh & Schulzke 2018). That drones, in the US public eye, also seem effective (variously defined) likely generates support as well (Kreps & Wallace 2016).

However, perceptions regarding the compliance of drone strikes with international humanitarian law can shape public attitudes. The public becomes less supportive of drone strikes when they are perceived to violate international law (Kreps 2014). Critiques of drone strikes in general are most salient with the public when they focus on legal issues rather than on questions of effectiveness (Kreps & Wallace 2016). While most of the research on public attitudes concerning drones uses samples of the American public, some research expands beyond America's borders, looking at countries such as Pakistan, which has been on the receiving end of US drone strikes (Fair et al. 2014). There is an opportunity for future research on drones and public opinion to connect more to behavioral research in international relations. One avenue could involve survey experiments evaluating the role of drones for surveillance, both domestic and international. China, for example, has used drones for internal surveillance.

Drone Proliferation

Another debate in the literature involves the proliferation of drones. Drones have spread rapidly around the world over the last decade and a half. Seventeen countries now have armed drones, and more than 100 countries have some kind of military drone program (Gettinger 2019). Countries such as the United States, China, and Israel have built their own drones. Others, such as Iraq, Nigeria, and Jordan, have purchased armed drones. Most countries with armed drones, including several US allies and partners, possess them due to Chinese exports. This could raise interesting research questions for the future concerning defense procurement and alliance politics (Spindel 2018).

There have been limited debates in this literature so far, mostly surrounding the likely extent of future proliferation and the consequences for international politics. As with other research on weapons proliferation (such as nuclear weapons), scholars seek to understand who will have access to what kinds of drones. There is a large gap in capabilities between short-range quadcopters designed for tactical surveillance missions over a few kilometers and MQ-9 Reapers that are controlled from across the world, via satellite, and carry AGM-Hellfire II air-to-ground missiles.

Gilli & Gilli (2016) are skeptical about the potential for drones to proliferate widely in a way that is relevant for the international security environment. They point out that using drones for global strike purposes, as the United States does, is incredibly complex, which limits the number of countries that can use drones in that fashion. This is one reason why even advanced European countries, such as the United Kingdom, Germany, and France, have imported drones from the United States rather than building their own—especially armed drones. Executing drone strikes over thousands of miles requires real-time access to satellite data and significant communications bandwidth, as well as the personnel and organizational systems required for systems integration. This will limit the number of countries that can use drones for over-the-horizon operations.

Fuhrmann & Horowitz (2017) show that, empirically, armed and advanced drones are spreading widely. They disaggregate drones into three broad categories: tactical systems, advanced systems, and armed systems (systems can be both advanced and armed). They show that security threats, and especially threats from militant groups, drive many countries to acquire advanced and armed drones. Democracies, seeking to reduce their own casualties, and autocracies, seeking to increase centralized control over the use of force, appear more likely to pursue armed drones, and more technologically sophisticated countries are more likely to acquire advanced drones (Fuhrmann & Horowitz 2017).

One way to integrate these findings and move forward is through more careful research on the potential for proliferation in the context of how countries will use drones. This could connect back to research on nuclear proliferation and how countries might seek to leverage nuclear weapons to improve their security situation (Gartzke & Jo 2007, Kroenig 2018, Sechser & Fuhrmann 2017, Singh & Way 2004). Countries seeking to use drones for over-the-horizon strikes may face significant operational constraints. Countries seeking to use drones tactically, or for shorter-range strike operations, may not face similar constraints. The security issues that most countries face are either internal—in the form of insurgencies or rebel movements of various types—or external but local, such as border disputes. For these types of missions, even a country with less sophisticated operational infrastructure and less advanced armed drones may be able to successfully utilize them. This is one path for future research.

Drones and Coercion

A final category of research on drones focuses on their potential utility for coercion. There have not been detailed debates between scholars in this context because most of the existing work, as explained above, represents applied theory. This work is based on classic research on coercion in international politics (for example, Schelling 1960) and seeks to understand how drones might influence deterrence, coercion, and compellence.

Key to work on drones and coercive outcomes are assumptions about technological advances that could make drones more credible as weapons in interstate wars. Authors imagine how further developments in military robotics, whether in the form of next-generation drones with more capabilities or swarms of drones, might shape coercion and warfare (Horowitz et al. 2016). Because drone strike capability changes the relative costs of war for the attacker and offers more certainty by increasing precision, countries with asymmetric advantages in the ability to use drones for strikes might be able to coerce potential adversaries in ways that have relevance for interstate war (Zegart 2018). This will be especially true as the capabilities of drones increase and they are better able to operate in contested airspace against adversaries with sophisticated air defenses.

Some observers fear that drones capable of targeted strikes, or even more, could soon be in the hands of many actors because the underlying technology is dual use. After all, the Islamic State and other nonstate actors have acquired simple armed drones. One concern is that acquisition of

advanced drones could lead to competition in military robotics and increase the risk of miscalculation as countries shoot each other's drones down (Boyle 2013). Others are less concerned, arguing that since drones, by definition, do not have a human in the cockpit, shooting them down is unlikely to uniquely trigger escalation between countries. In fact, what limited evidence exists about the shootdown of drones, including along the Syria–Turkey border, in the Kashmir region, and between the United States and Iran, suggests that countries will not react by escalating (Horowitz et al. 2016).

It is still early to draw broader inferences about drones and coercion, however. New, experimental results from war games suggest that elites are less likely to escalate in response to a drone being shot down than if an inhabited aircraft is shot down. As more countries with drones have crises and make escalation choices, the increase in data and cases will make it easier to do empirical research and advance knowledge.

CYBER

Few if any technology areas have attracted as much attention as the cyber realm in the twenty-first century. The Internet represented a four-trillion-dollar industry in 2016 even though only half of the world has Internet access (Nye 2017). Google Scholar analytics clearly demonstrate the rise of cyber as an area of research. For example, **Figure 1** shows that the number of articles indexed by Google Scholar using the terms cyberwar or cyber war rose from a little over 2,000 in 1999 to 4,400 in 2005, 8,330 in 2010, and 16,200 in 2018, the last available year with complete data. The numbers would be even higher if the figure reflected other ways scholars think about cyber, including cyber security, cyber deterrence, etc. Given the growth in scholarly interest, what does existing research suggest about how the cyber realm impacts international politics?

Since the early 1990s, scholars have studied how computer networks, in various forms, could function as weapons. Arquilla & Ronfeldt (1993) distinguished between cyberwar, which they regarded as occurring mostly between states, and netwar, which involves nonstate actors. Two decades later, Dombrowski & Demchak (2014, p. 88) described cyber capabilities as an "evolution

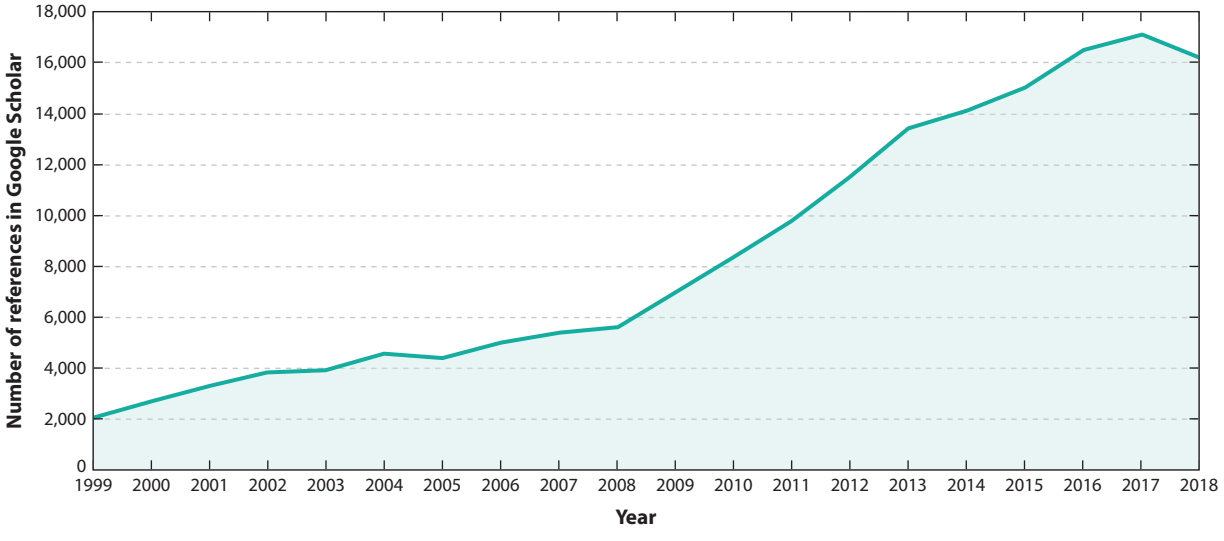

Figure 1

References to "cyber war" or "cyberwar" in articles indexed by Google Scholar, 1999–2018.

force, slowly altering the likely future conditions for interstate competition and the potential for kinetic forms of battle." Millions of cyber attacks occur every day around the world, but in contrast to kinetic uses of force, their legal and political status is unclear. Since cyber attacks can have consequences that range from irritation to physical destruction and the loss of life, they are complicated legally (Schmitt 2011). Cyber attacks can also occur via multiple means, including network connections, supply chains that eventually link to networks, or insider attacks (Nye 2017).

Another complication is that, while cyber tools can be used as weapons, they are not necessarily weapons. Cyber applications occur in multiple areas that roughly correspond to areas in the kinetic world, and also overlap. One way that actors use cyber tools is for purposes that roughly mirror criminal activity in the physical world. Instead of physically robbing a bank, for example, an individual or group might hack into a bank to steal money or information.

A second way for actors to use cyber roughly mirrors the intelligence world. Nonstate actors and countries attempt to steal information, disrupt potential adversaries, and the like. For example, in the 2014 North Korean hack of Sony Pictures, instead of North Korean personnel physically accessing Sony headquarters and stealing papers or copying electronic files, North Korean hackers allegedly used cyber tools to achieve the same result.

A third way in which actors use cyber mirrors kinetic military activity. Clear military uses of cyber include efforts to attack adversary military networks to shut them down and make it harder for them to operate their forces in a conflict. Other military uses of cyber could include hacking into an adversary computer network to shut down an integrated air defense system as opposed to bombing that system. The goal is to achieve air superiority; the tool could be from the cyber realm, or not.

Several issues influence the growing literature on cyber in international politics. First, the newness of the cyber domain relative to, say, land or sea means that scholars and policy makers lack deep historical knowledge and a clear set of analogies to shape how they think about the consequences of cyber activities (Slayton 2017). There are also questions about whether cyber should even be considered a domain. Second, cyber operations are highly technical, and understanding them requires detailed knowledge of programming and networks. Most policy makers and international relations scholars have limited training in these areas. Third, because of cyber's virtual character, it is difficult to effectively measure either the balance of cyber capabilities or the effectiveness of most cyber attacks (Schneider 2019a). Fourth, unless a group or country either claims responsibility or is outed by a target, much cyber activity remains more covert than kinetic actions (though some kinetic actions can be covert, of course) (Poznansky & Perkoski 2018).

These research design and informational challenges combine to complicate the systematic study of cyber's role in international politics. As time passes, more available information on cyber interactions between countries and cyber postures will help resolve these issues.

How Transformational Is Cyber in International Security?

One existing debate in the literature, though it is more between the policy world and academia than between academics, is whether cyber is a game-changing technology for the international security environment. How important is cyber war? Many policy makers believe that the cyber domain is critical, drawing on such examples as Russia's cyber operations against Estonia and Georgia as well as concerns about cyber vulnerabilities for militaries and critical infrastructure. For example, in 2012, former US Secretary of Defense Leon Panetta spoke about a "cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life" (Panetta 2012).

To some extent, the debate about the importance of cyber in international politics revolves around the definition of what constitutes cyber war. If cyber war is specifically the use of

computer-based attacks to generate effects on the ground previously generated by kinetic weapons systems, that is a limited definition when it comes to measuring effects (though a clear definition). Alternatively, one could define cyber war or cyber conflict more broadly to include interactions that happen entirely in the digital realm but that have consequences for the balance of power and international conflict.

Some scholars argue that cyber capabilities could have significant consequences for international security. Cyber capabilities, by blurring the lines between war and peace given the increased potential for nonlethal attacks, could widen the scope of war (Kello 2013). Countries relying on networks for computer and economic power are inherently at risk of that reliance being exploited. Particularly vulnerable are governments and militaries that view network access and bandwidth as essential for everything from intelligence to logistics to battlefield operations (Libicki 2009).

The constant character of cyber intrusions and the lack of clear standards, based on history, concerning the scope of cyber conflict could make signaling in the cyber domain especially difficult. Some scholars argue that this ambiguity could increase the risk of escalation in a crisis (Lin 2012). Moreover, the ability of cyber tools to generate economic harm and disrupt military networks could have significant second-order consequences, especially given the ease of access many actors could have to these tools, as well as challenges surrounding attribution of cyber attacks (Kello 2013). Regardless of the reality, policy makers believe there is an offensive advantage in cyberspace, which could generate biases in favor of offensive military cyber operations (Junio 2013, p. 130). Bureaucratic politics could also make cyber war more likely. Due to principal–agent problems that make complete control difficult, and the belief of attackers that they can keep cyber conflicts from escalating into the kinetic realm, cyber wars may be more likely than traditional conflicts (Junio 2013).

Most scholars working on cyber issues, however, argue that cyber capabilities are unlikely to be critical to warfare (Junio 2013, Rid 2012). To some extent, that conclusion is based on a definition of cyber war limited to military capabilities that cause kinetic consequences, but the argument is broader. These scholars have concluded that the worst-case fears of policy makers regarding the transformational character of cyber war are overblown (for example, see Rid 2013). This is interesting for academic reasons and because it demonstrates a gap in perceptions between academics and policy makers about the ultimate risks from cyber conflict. An analysis of cyber incidents and disputes from 2001 through 2014 shows that countries do not often use cyber attacks, and when they do, they use them in low-intensity ways that are unlikely to cause escalation (Valeriano & Maness 2015). Liff (2012) predicts that while computer network attacks will occur constantly, high-level cyber attacks that change the probability of escalation will be rare. The reason is political. The cases where cyber attacks are most likely to appear to influence the probability of escalation are those in which countries already have a strategic and political reason to escalate. Thus, it is politics and the breakdown of bargaining that are leading to conflict; cyber attacks are simply the tool (Liff 2012). This conclusion connects work on cyber to broader research on deterrence and coercion.

The critique of cyber as transformational extends to the most infamous use of cyber capabilities for intelligence or military purposes: the Stuxnet attack on Iran's nuclear enrichment program. The attack occurred in 2010 and gained prominence as one of the first computer network attacks known to cause kinetic damage. Lindsay (2013) argues that while many scholars and analysts initially used the attack to illustrate the revolutionary potential of cyber capabilities, in fact the attack shows the opposite. The Stuxnet attack worked only because the attacker (the United States) had significant capabilities and, in combination with an ally (Israel), used traditional intelligence methods to infect Iran's centrifuge program.

Similarly, Lindsay (2015) points out a gap between China's ambitions to threaten critical Western infrastructure during a conflict through cyber attacks and the likely reality. He argues that there is a cyber version of the stability–instability paradox. Cyber attackers keep the costs of attacks below the level at which they would provoke retaliation—excluding retaliation in the cyber realm.

Turning back to the different applications of cyber capabilities to international relations, even if cyber is not as transformational as the policy world and some academics originally believed, cyber capabilities could still have significant consequences for international politics. Russia's 2016 US election actions, for example, certainly sowed distrust and confusion in a way that achieved Russia's goals. Cyber capabilities are more likely to have relevance as a method of espionage and crime, used for economic activities and attacks on softer targets. Cyber attacks could serve as political and economic instruments and as complements to intelligence activity. Cyber capabilities could also play a useful role in coercion in international politics, complementing traditional kinetic tools (Valeriano et al. 2018).

One possibility for future research that could bridge international political economy and international conflict is work on the politics of cyber strategies and their impact on international economics. Just as cyber attacks can be used against militaries or intelligence services, cyber attacks can disrupt economic transactions within borders or across borders. Cyber attacks against critical infrastructure and important private companies also raise questions for scholars of politics about public–private coordination. Most research on this topic up to this point has occurred outside of political science (for example, see Hua & Bapna 2013), but there is an opportunity for political science research here as well.

As described below in the discussion of cross-domain deterrence, another response to the research on cyber and international security is a focus on cyber in the context of other domains of warfare, which also has the benefit of integrating research on cyber into more general international politics research.

Cyber Offense Versus Defense

Do cyber capabilities inherently advantage the attacking side? There has been a notion that anyone with a computer and an Internet connection could be a hacker who causes damage. Similarly, some policy makers fear that cyber could disrupt international politics because it is available at low cost to smaller states and nonstate actors (Panetta 2012).

Critical to the notion of cyber as disruptive to existing power balances is the idea that cyber attacks are both easy to perform and hard to defend against. If the offense can attack constantly and the defense must have a 100% success rate, it would seem to logically follow that a cyber-dominant world is an offense-dominant world.

Yet, this is another area where most international relations research suggests that fears are exaggerated. Again, there is less debate in the academic literature than between academia and some policy makers. The reason has to do with the conflation of being able to acquire any cyber capabilities with being able to acquire advanced cyber capabilities. Basic systems are easy to develop, but sophisticated systems require computing and infrastructure capabilities that are more difficult to design and operate (Liff 2012). Countries with a lot to lose in the cyber arena are also investing significantly in defense.

One key insight in the discussion of cyber offense and defense involves the importance of organizations in both carrying out cyber attacks and defending against them. It is no longer true, and probably never was, that anyone with a computer can successfully launch a cyber attack against a state or sophisticated organization. Additional requirements include skill and operational capacity. Skill refers to the underlying training and knowledge of the attackers. Operational capacity refers

to abilities like scanning, managing network access, updating software, and effectively operating complex cyber systems in a world of uncertainty (Slayton 2017). It therefore may make more sense to think about cyber capabilities in terms of a balance of capabilities between two actors rather than as inherently favoring the offense or defense. Just as the United States has superior conventional military forces to Botswana, the United States also has superior cyber capabilities to Botswana. This would suggest for research a balance-of-forces approach comparable to approaches taken for studying other types of military capabilities.

Gartzke & Lindsay (2015) further argue that offense is not even necessarily cheaper in the cyber domain. The need for attacks to stay covert in situations short of war imposes operational limitations, while defenders can use forms of concealment and spoofing to try to deceive attackers.

Some scholars are now trying to incorporate these issues directly into their studies. Garfinkel & Dafoe (2019) argue that when investment levels are low, the offense benefits in the cyber domain, but that this reverses as investments grow. Their focus on evaluating zero-day exploits of computer networks represents a methodological advance in the literature due to its specificity. Their model shows that as vulnerabilities in computer networks increase, they are discovered by defenders through investments, and eventually defenders can reach network protection saturation—blunting the offense advantage at lower levels of investment.

Cyber Deterrence

Is deterrence possible in cyberspace, whether between states or involving nonstate actors? The conventional wisdom in the policy world is that cyber deterrence is extremely difficult. This relates to the attribution problem—if it is possible to launch cyber attacks without being detected, what generates the fear of being caught that generates deterrence?

The attribution problem itself has been a focus of the cyber literature in international relations. This is an area where interdisciplinary work and collaborations with computer science and other fields are helpful. The basic question is whether defenders can know who is launching cyber attacks at a confidence level that enables them to respond. Note that the standard of proof for attribution in international politics may differ from that required for international domestic or legal purposes, at least in a country like the United States with a strong commitment to the rule of law. Say, for example, a country is satisfied, based on computer forensic investigations, that it knows the location of its attacker. If that location is a military base in a country that is a potential adversary, the attacked country may not need additional information to be confident in attribution. If the traced location of the attack is some public location, that is a different story. However, as cyber sophistication has grown, so has the difficulty of launching successful attacks against well-defended cyber institutions from a laptop on a public network.

More generally, advances in attribution limit the deception advantages for cyber attackers, while defenders can also use deception to try to entrap attackers—both defeating an attack and identifying the attacker (Gartzke & Lindsay 2015).

Strong defensive capabilities require attackers to use resources and energy in an attack, which may generate some degree of deterrence by denial in cyberspace (Nye 2017). This form of deterrence could be especially effective for criminals and nonstate actors. Other scholars might argue that there is the potential for deterrence by punishment, through sanctions once attribution occurs or through "hacking back" once defenders discover the identity of attackers. Hacking back may not always be a successful strategy, however. A country may not want to say that it knows the identity of an attacker for fear of revealing cyber intelligence capabilities to potential adversaries.

One promising area of research is cross-domain deterrence. Cross-domain deterrence research focuses on how capabilities in one domain, such as cyber, influence other domains, such as land

(Gartzke & Lindsay 2019). There are a multitude of potential cross-domain challenges to investigate, and more empirical research is possible by framing questions in ways that might include more historical cases.

Cyber Norms

Scholars have also tackled questions of norm development in the cyber arena. Is the evolution of cyber-specific norms, or even laws, necessary or desirable? From one perspective, cyber attacks are, conceptually, subject to the same legal restrictions as kinetic attacks. On the other hand, the lack of an agreed-upon definition for cyber attacks or cyber war, as well as the continuous nature of some attempts at cyber intrusions, makes such restrictions hard to elucidate.

Most of the research on cyber norms is necessarily normative—no pun intended—given that international efforts to promote cyber cooperation have faced roadblocks. Countries have not agreed on international rules surrounding cyber attacks or cyber war, and such incidents as Russia's cyber intrusions during the 2016 US presidential election cycle have made progress unlikely through formal international channels in the short term. Yet, in other areas, such as nuclear weapons, countries have been able to come to agreements despite significant political tension. Work that creates conceptual space for cyber norms exists (Finnemore & Hollis 2016), but there is room for new empirical research. One promising avenue could involve comparative case studies: Efforts to create international cyber rules of the road would be compared to analogous efforts when other domains were new, such as airpower in the early twentieth century.

ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) represents the ability of computers and machines to complete tasks previously thought to require human intelligence. It is useful to distinguish so-called narrow AI from artificial general intelligence (AGI). Narrow AI is defined as discrete algorithms designed to execute a specific task, such as classifying a type of image or playing a game. An example is AlphaGo, the algorithm developed by DeepMind that defeated one of the world's best Go players in 2016. A machine with AGI, in contrast, could innovate on its own—not just executing a specific task but teaching itself to do new tasks in new categories of activities. Countries and companies around the world believe that advances in AI could profoundly shape international politics. China's National AI strategy suggests that leadership in AI will be critical to national power, and the US Congress created a National Security Commission on Artificial Intelligence to develop policy ideas that will ensure continued US leadership. Most research on the consequences of advances in AI for international politics focuses on narrow AI.

Scholarship in political science on AI is still in early stages, so clear debates have not yet emerged. Most applications of AI to militaries are still in their infancy, and most applications of algorithms for militaries will be in areas such as logistics and training rather than close to or on the battlefield (Cummings 2017). That being said, some scholars have attempted to apply existing theory to study how AI could shape international politics (Jensen et al. 2019). Approaches include using research on military innovation (Horowitz 2018), Offense–Defense theory (Garfinkel & Dafoe 2019), and strategic stability (Altmann & Sauer 2017, Horowitz et al. 2019), among others. This will be a growing area for scholarship moving forward, though it will face the same empirical limitations identified at the outset of this article.

CONCLUSION

Critical to research on how emerging technologies are shaping the international security environment will be the ability of scholars to connect this research to traditional academic questions in

international relations and explain how these advances impact topics of traditional interest, such as deterrence and war. As countries and militant groups continue integrating emerging technologies into their military capabilities, scholarship on these topics will become even more important. Drones, for example, represent just the tip of the spear in potential applications of military robotics.

There are several promising areas of research in the area of military robotics. One question is whether drone capabilities spread in an asymmetric or relatively symmetric fashion. If countries have the ability to threaten each other with drones, for example, it could lead to a kind of deterrence in the context of strikes against leadership, even as drones become more regular parts of military arsenals. Another question is whether the use of drones makes war and the use of force in general more likely. Some fear that drones make war too easy, which means leaders will be more likely to employ force (Boyle 2013). While empirical evidence on this point is limited, more will likely become available in the coming years, given how many countries now possess armed drones. A final question for future research concerns regime type and the military use of drones. While most research has focused on democracies, where casualty aversion explains public support for drones, autocrats may also favor drones, but for different reasons. Autocratic regimes, almost by definition, do not trust large segments of their population, and drones are easier to control because the pilots are on the ground in a location a regime can monitor. The theoretically improved ability to monitor the use of force could be very attractive for autocrats and have effects on domestic repression and interstate war. This could be an interesting area of research, both from a principal–agent perspective and empirically, in the years ahead.

As more scholars examine the intersection of cyber and international politics, research in this area will likely evolve as well. One potential evolution would involve more use of game theoretic models to understand incentives for using cyber capabilities, or not, in particular situations. Moreover, as additional evidence becomes publicly available about particular cyber attacks and national cyber strategies, in-depth research on a larger number of cyber topics will become plausible within political science. Questions of cyber and escalation to the kinetic world could grow in prominence, especially as scholars use methods such as war games to test how actors will think about responding to cyber attacks in a crisis situation (Schneider 2019b).

Several areas in which scholarship has been limited up to this point could be primed for further investigation. Some possibilities referenced above include synthetic biology, hypersonics, and additive manufacturing. Another promising area for research is outer space (Dolman 2002, Early 2014). Perhaps due to a perception that too much information involved in space policy is classified, many scholars have shied away from studying what influences how countries and militaries use outer space. However, more is available than many people think. Given the growing importance of space for militaries, space should be the subject of growing research.

Overall, the intersection of emerging technologies and international politics will continue to be a critical area of investigation in the years ahead.

DISCLOSURE STATEMENT

The author is not aware of any affiliations, memberships, funding, or financial holdings that might be perceived as affecting the objectivity of this review.

LITERATURE CITED

Altmann J, Sauer F. 2017. Autonomous weapon systems and strategic stability. *Survival* 59:117–42
Arquilla J, Ronfeldt D. 1993. Cyberwar is coming! *Comp. Strategy* 12:141–65

Biddle SD. 2004. *Military Power: Explaining Victory and Defeat in Modern Battle*. Princeton, NJ: Princeton Univ. Press

Boyle MJ. 2013. The costs and consequences of drone warfare. *Int. Aff.* 89:1–29

Byman D. 2013. Why drones work. *Foreign Aff.* 92:32–43

Cronin AK. 2013. Why drones fail. *Foreign Aff.* 92:44–54

Cummings ML. 2017. *Artificial intelligence and the future of warfare*. Res. Pap., Chatham House, Royal Inst. Int. Aff., London, UK. **https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings.pdf**

Dolman EC. 2002. *Astropolitik: Classical Geopolitics in the Space Age*. Portland, OR: Frank Cass

Dombrowski P, Demchak CC. 2014. Cyber war, cybered conflict, and the maritime domain. *Naval War Coll. Rev.* 67:70–96

Drezner DW. 2019. Technological change and international relations. *Int. Relat.* 33:286–303

Early BR. 2014. Exploring the final frontier: an empirical analysis of global civil space proliferation. *Int. Stud. Q.* 58:55–67

Fair CC, Kaltenthaler K, Miller WJ. 2014. Pakistani opposition to American drone strikes. *Political Sci. Q.* 129:1–33

Fearon JD. 2018. Cooperation, conflict, and the costs of anarchy. *Int. Organ.* 72:523–59

Finnemore M, Hollis DB. 2016. Constructing norms for global cybersecurity. *Am. J. Int. Law* 110:425–79

Fuhrmann M, Horowitz MC. 2017. Droning on: explaining the proliferation of unmanned aerial vehicles. *Int. Organ.* 71:397–418

Garfinkel B, Dafoe A. 2019. How does the offense–defense balance scale? *J. Strategic Stud.* 42:736–63

Gartzke E, Jo D-J. 2007. Determinants of nuclear weapons proliferation: a quantitative model. *J. Confl. Resolut.* 51:167–94

Gartzke E, Lindsay JR. 2015. Weaving tangled webs: offense, defense, and deception in cyberspace. *Secur. Stud.* 24:316–48

Gartzke E, Lindsay JR. 2019. *Cross-Domain Deterrence: Strategy in an Era of Complexity*. New York: Oxford Univ. Press

Gettinger D. 2019. *The drone databook*. Cent. Stud. Drone, Bard College, Annandale-on-Hudson, NY. **https://dronecenter.bard.edu/projects/drone-proliferation/databook/**

Gilli A, Gilli M. 2016. The diffusion of drone warfare? Industrial, organizational and infrastructural constraints: military innovations and the ecosystem challenge. *Secur. Stud.* 25:50–84

Gilli A, Gilli M. 2019. Why China has not caught up yet: military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage. *Int. Secur.* 43:141–89

Horowitz MC. 2010. *The Diffusion of Military Power: Causes and Consequences for International Politics*. Princeton, NJ: Princeton Univ. Press

Horowitz MC. 2016. Public opinion and the politics of the killer robots debate. *Res. Politics* 3:1–8

Horowitz MC. 2018. Artificial intelligence, international competition, and the balance of power. *Texas Natl. Secur. Rev.* 1:37–57

Horowitz MC, Kreps SE, Fuhrmann M. 2016. Separating fact from fiction in the debate over drone proliferation. *Int. Secur.* 41:7–42

Horowitz MC, Kreps SE, Fuhrmann M. 2019. Yes, Iran shot down a U.S. drone. Here's why you (still) don't need to worry. *Washington Post/Monkey Cage Blog*, June 20. **https://www.washingtonpost.com/politics/2019/06/20/yes-iran-shot-down-us-drone-heres-why-you-still-dont-need-worry/**

Hua J, Bapna S. 2013. The economic impact of cyber terrorism. *J. Strateg. Inf. Syst.* 22:175–86

Jensen BM, Whyte C, Cuomo S. 2019. Algorithms at war: the promise, peril, and limits of artificial intelligence. *Int. Stud. Rev.* **https://doi.org/10.1093/isr/viz025**

Jervis R. 1989. *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*. Ithaca, NY: Cornell Univ. Press

Johnston PB. 2012. Does decapitation work? Assessing the effectiveness of leadership targeting in counterinsurgency campaigns. *Int. Secur.* 36:47–79

Johnston PB, Sarbahi AK. 2016. The impact of U.S. drone strikes on terrorism in Pakistan. *Int. Stud. Q.* 62:203–19

Jordan J. 2009. When heads roll: assessing the effectiveness of leadership decapitation. *Secur. Stud.* 18:719–55
Jordan J. 2014. Attacking the leader, missing the mark: why terrorist groups survive decapitation strikes. *Int. Secur.* 38:7–38
Junio TJ. 2013. How probable is cyber war? Bringing IR theory back in to the cyber conflict debate. *J. Strateg. Stud.* 36:125–33
Kello L. 2013. The meaning of the cyber revolution: perils to theory and statecraft. *Int. Secur.* 38:7–40
Kilcullen D, Exum A. 2009. Death from above, outrage down below. *New York Times*, May 16. **https://www.nytimes.com/2009/05/17/opinion/17exum.html**
Koblentz GD. 2011. *Living Weapons: Biological Warfare and International Security*. Ithaca, NY: Cornell Univ. Press
Kostyuk N, Zhukov YM. 2019. Invisible digital front: Can cyber attacks shape battlefield events? *J. Confl. Resolut.* 63:317–47
Kreps SE. 2014. Flying under the radar: a study of public attitudes towards unmanned aerial vehicles. *Res. Politics* 1:1–7. **https://doi.org/10.1177/2053168014536533**
Kreps SE, Wallace GP. 2016. International law, military effectiveness, and public support for drone strikes. *J. Peace Res.* 53:830–44
Kroenig M. 2018. *The Logic of American Nuclear Strategy: Why Strategic Superiority Matters*. New York: Oxford Univ. Press
Libicki MC. 2009. *Cyberdeterrence and Cyberwar*. Washington, DC: RAND Corp.
Liff AP. 2012. Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war. *J. Strateg. Stud.* 35:401–28
Lin H. 2012. Escalation dynamics and conflict termination in cyberspace. *Strateg. Stud. Q.* 6:46–70
Lindsay JR. 2013. Stuxnet and the limits of cyber warfare. *Secur. Stud.* 22:365–404
Lindsay JR. 2015. The impact of China on cybersecurity: fiction and friction. *Int. Secur.* 39:7–47
Mir A. 2018. What explains counterterrorism effectiveness? Evidence from the US drone war in Pakistan. *Int. Secur.* 43:45–83
Mir A, Moore D. 2019. Drones, surveillance, and violence: theory and evidence from a US drone program. *Int. Stud. Q.* 63:846–62
Nye JS Jr. 2017. Deterrence and dissuasion in cyberspace. *Int. Secur.* 41:44–71
Panetta LE. 2012. Remarks by Secretary Panetta on cybersecurity to the Business Executives for National Security, New York City, Oct. 11. **https://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136**
Poznansky M, Perkoski E. 2018. Rethinking secrecy in cyberspace: the politics of voluntary attribution. *J. Glob. Secur. Stud.* 3:402–16
Rid T. 2012. Cyber war will not take place. *J. Strateg. Stud.* 35:5–32
Rid T. 2013. *Cyber War Will Not Take Place*. New York: Oxford Univ. Press
Schelling TC. 1960. *The Strategy of Conflict*. Cambridge, MA: Harvard Univ. Press
Schmitt MN. 2011. Cyber operations and the jud ad bellum revisited. *Villanova Law Rev.* 56:569–606
Schneider J. 2019a. The capability/vulnerability paradox and military revolutions: implications for computing, cyber, and the onset of war. *J. Strateg. Stud.* 42:841–63
Schneider J. 2019b. *Cyber and crisis escalation: insights from wargaming*. Work. Pap., Mario Einaudi Cent. Int. Stud., Cornell Univ. **https://pacs.einaudi.cornell.edu/sites/pacs/files/Schneider.Cyber%20and%20Crisis%20Escalation%20Insights%20from%20Wargaming%20Schneider%20for%20Cornell.10-12-17.pdf**
Sechser TS, Fuhrmann M. 2017. *Nuclear Weapons and Coercive Diplomacy*. New York: Cambridge Univ. Press
Sechser TS, Narang N, Talmadge C. 2019. Emerging technologies and strategic stability in peacetime, crisis, and war. *J. Strateg. Stud.* 42:727–35
Shah A. 2018. Do U.S. drone strikes cause blowback? Evidence from Pakistan and beyond. *Int. Secur.* 42:47–84
Singh S, Way CR. 2004. The correlates of nuclear proliferation—a quantitative test. *J. Confl. Resolut.* 48:859–85
Slayton R. 2017. What is the cyber offense-defense balance? Conceptions, causes, and assessment. *Int. Secur.* 41:72–109

Smith M, Walsh JI. 2013. Do drone strikes degrade Al Qaeda? Evidence from propaganda output. *Terrorism Political Violence* 25:311–27

Spindel J. 2018. *Beyond military power: the symbolic politics of conventional weapons transfers*. PhD Diss., Dep. Political Sci., Univ. Minn.

Talmadge C. 2019. Emerging technology and intra-war escalation risks: evidence from the Cold War, implications for today. *J. Strateg. Stud.* 42:864–87

Valeriano B, Jensen BM, Maness RC. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York: Oxford Univ. Press

Valeriano B, Maness RC. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford Univ. Press

Volpe TA. 2019. Dual-use distinguishability: how 3D-printing shapes the security dilemma for nuclear programs. *J. Strateg. Stud.* 42:814–40

Walsh JI, Schulzke M. 2018. *Drones and Support for the Use of Force*. Ann Arbor: Univ. Mich. Press

Williams H. 2019. Asymmetric arms control and strategic stability: scenarios for limiting hypersonic glide vehicles. *J. Strateg. Stud.* 42:789–813

Zegart A. 2018. Cheap fights, credible threats: the future of armed drones and coercion. *J. Strateg. Stud.* **https://doi.org/10.1080/01402390.2018.1439747**