CISSM | CENTER FOR INTERNATIONAL & SECURITY STUDIES AT MARYLAND

Double or Nothing? The Effects of the Diffusion of Dual-Use Enabling Technologies on Strategic Stability

By Alexander H. Montgomery

CISSM Working Paper

July 2020

This paper was made possible with funding from the Carnegie Corporation of New York.

Center for International
and Security Studies at Maryland
4113 Van Munching Hall,
School of Public Policy, University of Maryland
College Park, MD 20742
(301) 405-7601

SCHOOL OF PUBLIC POLICY
CENTER FOR INTERNATIONAL & SECURITY STUDIES AT MARYLAND

Abstract

Left unchecked, the diffusion of dual-use enabling technologies—such as additive manufacturing, artificial intelligence, and advanced communication technologies—may pose threats to strategic stability. The rapid development of these technologies by the United States and its allies and partners has taken place primarily in the private sector, and is largely stored and transported in easily-diffused digital formats. If diffusion occurs, it could lead to significant innovation in, or even transformation of, competitors' military forces. Enabling technologies can be particularly dangerous since they can have a feedback effect by accelerating innovation itself. Rapid shifts in the balance of military forces due to adoption of these technologies by competitors can, in turn, threaten strategic stability. To counter these threats, the United States and its allies and partners need a common awareness of the factors that enable and constrain technological diffusion, adoption, and transformation. In order to deepen understanding of how these developments are most likely to impact international security and contribute to the creation of mitigating policies, this paper develops a model of the pathways through which enabling technologies could affect strategic stability, drawing on the literatures on technological invention, innovation, and evolution; nuclear proliferation; and conventional arms flows. Diffusion of inventions can occur through four pathways: buy, beg, steal or copy; yet none of these pathways guarantee successful diffusion of technological inventions, and are subject to a variety of countermeasures. Moreover, there are significant downstream hurdles to adopting these technologies and using them to transform military forces. Consequently, while some diffusions may have a significant multiplicative effect, many may have little or no net effect on strategic stability. Policymakers must carefully and consider specific technologies and strategically act to effectively limit those that pose the greatest danger.

Introduction

The current search for a "competitive edge" in military power has led to an increase in demand for novel inventions from the civilian sector. Such technologies are ripe for diffusion due to their dual-use nature and digital formats. The strategic implications of increased demand for these inventions is of primary concern when diffusion could lead to significant military innovation by a competitor. Military innovations that help to significantly close capability gaps between competitors and U.S. and allied forces; spark rapid evolutionary changes in force structure, deployment, or employment; or are otherwise connected to ongoing or potential military revolutions are particularly threatening. These changes can, respectively, result in decreasing, eliminating, or even reversing U.S. power advantages under certain conditions. Shifts in the balance of power due to such innovations threaten strategic stability, increasing the probability of war.[1] Consequently, the focus of this paper is on emerging dual-use inventions that could lead to innovations, rapidly evolve competitor capabilities, and threaten strategic stability through alterations in the balance of forces.[2]

Invention is "the generation of something new: a new object, product, process, design, functionality or material not previously available." However, inventions themselves do not drive change unless they are adopted. An *innovation* is a "successful or adopted invention" that is "put into production or wide-spread use, or [is] selected and thus leave[s] an evolutionary footprint." This paper is concerned with inventions and innovations that are *technologies*, "ideas about how to re-arrange matter, energy and information; …means to fulfill human needs; …[and] artifacts, devices, methods and materials available to humans to accomplish specific tasks."[3] *Enabling* technologies such as steam engines, the internal combustion engine, semiconductors, and the internet are some of the most important inventions, since they accelerate innovation itself and are applicable across a number of sectors.[4] These technologies, the knowledge that underlies them, and artifacts based on them are in inherently *dual-use*, i.e., "technologies intended for civilian application that can also be used for military purposes."[5] Dual-use enabling technologies are consequently among the most important ones to attempt to safeguard. Single-use military technologies, i.e., those that are developed for military purposes and lack civilian applications, are also crucial to safeguard. Safeguarding the latter is also easier due to many factors, including classification requirements and a highly restricted set of applications. Indeed, this paper draws on the diffusion of single-use technologies as examples, and some of the recommendations apply to both types of technologies. Arms control regimes and governments, however, typically focus on limiting the spread of military technologies, with limited (and failed) exceptions such as high-performance computing and encryption.

---

[1] See Bas and Coe 2012; for articles related to specific technologies, see Sechser, Narang, and Talmadge 2019.
[2] Balance of forces here includes force structure, deployment, and employment: together, force posture.
[3] Definitions of invention, innovation, and technologies from Santa Fe Institute Events 2016. Defining these terms is a well-scarred battlefield; they are defined this way here so as to set up a clear ordering from invention to innovation and from there to some degree of evolutionary technological change. This ordering is generally uncontroversial; see Ruttan 1959, cited in Parayil 1991, cf. Padgett and Powell 2012, 5.
[4] Enabling technologies are also known as general-purpose technologies. Bresnahan and Trajtenberg 1995, 83–84.
[5] National Research Council 2004, 18, cited in Forge 2010.

This paper focuses on the spread of dual-use enabling technologies not only due to a relative lack of policy attention but also due to the positive feedback loop created by adoption of these technologies, which makes them more likely to spur further innovations and consequently transform systems. Many of these enabling technologies have been driven by military and defense-related demand.[6] While it is impossible to predict precisely which technologies are likely to qualify as enabling technologies, prime candidates include a small set of inventions that are frequently associated with the vanguard of military-relevant research. These include additive manufacturing (AM), artificial intelligence (AI), and technologies that underpin advanced sensing and communication. None of these are "new" inventions per se—AM has been used since the 1980s,[7] the first machine learning program was created in 1952,[8] and many of the underpinnings of advanced sensing and communications technologies, such as frequency-hopping and high-frequency transmission and reception, were invented in World War II.[9] Indeed, it has taken decades for some of these inventions to result in true innovation, and whether these innovations have led to transformation of military forces in turn is still unclear.[10]

Safeguarding militarily-relevant technologies has always been difficult: export controls can only do so much to prevent their spread. Moreover, most technologies can be developed indigenously (i.e., with minimal outside help), although it can take decades for technological catch-up through indigenous development to happen. Existing export control regimes typically work by generating a "trigger list" of items that could be used to carry out prohibited activities. Suppliers of these list items voluntarily agree to implement domestic regulations prohibiting the sale of these dual-use items to those who may potentially use them to create weapons, equip an illegal facility, or subsequently transfer the technology to malignant end users, such as violent extremists. Additional obligations require regulation at the level of border controls and the use of law enforcement as well as export certification, and generally rely on the physical interdiction of technologies. The nuclear export control regime in particular has been strengthened multiple times after significant lapses, particularly after the discovery of Iraq's clandestine program after the Gulf War and the A.Q. Khan network.[11] Despite these controls, it is still possible for countries to develop nuclear and other technologies indigenously given a sufficient technological base, determination, and time: North Korea took 20–25 years to develop nuclear weapons despite being a prime target identified by export control regimes.[12]

It is already exceedingly difficult for existing regimes to keep pace with evolving technologies. The digitization of these technologies makes diffusion much more difficult to stop (or even slow), particularly for conventional dual-use items.[13] Nevertheless, existing dual-use export control regimes are well-developed for nuclear weapons and precursor materials (Nuclear Suppliers Group), chemical and biological weapons (Australia Group), some means of delivery (Missile Technology Control Regime), and major conventional weapons (Wassenaar Arrangement). However, regimes for cyber and space weapons are, by contrast, non-existent,

[6] Ruttan 2006, 166.
[7] Nelson 2015.
[8] McCarthy 1990.
[9] Kiesler and George 1942; Purcell, Montgomery, and Montgomery 1952.
[10] Krepinevich 2002.
[11] Blackford 2005.
[12] Montgomery 2013.
[13] Nelson 2019.

and informal agreements and non-binding political ones have borne little fruit. None of these regimes have developed robust procedures to counter the threat of diffusion posed by digitization of dual-use technologies.

To counter this threat and mitigate risk from the diffusion of enabling dual-use technologies, the United States and its allies and partners need a common understanding of the process through which technology can spread, be adopted, and eventually transform military systems. This process can be modeled as a series of steps. Separating the diffusion of an invention from the adoption of the invention into existing systems (i.e., innovation) has a number of advantages. First, inventions rather than innovations diffuse: the actual items that are being diffused (whether substantial or not) are, at best, whole inventions and, more typically, are parts of inventions, whether in the form of artifacts, explicit knowledge, or (rarely) tacit knowledge. This is because innovations are embedded in systems that rely on implicit local conditions that are often incompatible with the target environment.[14] Second, while inventions may be relatively consistent in form, innovations can have very different forms that depend on context due to the need to fit inventions into existing systems. Third, the problem of diffusion and the problem of adoption have different causes and effects—and consequently, different weaknesses that can be targeted to potentially contain and reduce the spread and adoption of technologies.

Fortunately, the diffusion of invention does not inevitably lead to innovations, nor does the diffusion of innovations inevitably lead to game-changing revolutionary leaps. A military-technical "revolution" requires both technology adoption and transformation (including systems development, operational innovation, and organizational adaptation).[15] Depending on how well an innovation is integrated with an actor's overall systems, integration may lead to outcomes short of revolution, ranging from rapid but still contained evolution to small and incremental change or even no progress. In some cases, it can even lead to devolution. Technologies may be ill-suited for the recipient actor due to lack of necessary financial capital, indigenous materials, supporting technologies, or domestic expertise; systems or operational incompatibility; or lack of organizational capital or flexibility. In these cases, diffusion may end up placing those actors on suboptimal or even retrograde technological trajectories.[16] Thus, even if technologies turn out to be compatible and are successfully adopted by some elements of the military by, for example, swapping new weaponry into existing systems, this may have little effect on a country's forces unless systems, operational approaches, and organizational structures are fully aligned with the innovations.

The net effect of diffusion is difficult to properly measure. The actual or potential trajectory must be carefully compared to a plausible counterfactual: absent diffusion, would the actor have indigenously produced or adopted an invention in any case? For example, China originally planned on using plutonium in its nuclear program for its first weapon rather than highly-enriched uranium (HEU). Assistance provided by the Soviet Union later led to a shift to an HEU program. Analysis indicates that China could have tested its own indigenous plutonium bomb around the same time absent Soviet help.[17]

[14] Meshkati 1989
[15] Krepinevich 1994, 2002.
[16] Montgomery and Volpe 2017.
[17] Yanqiong and Jifeng 2009.

The process by which inventions are diffused will also influence the likelihood of successful change. For example, even in historical cases where nuclear weapons-related technologies were directly and intentionally transferred, few seem to have accelerated the development of nuclear weapons by the recipient countries.[18] Less-efficient or indirect transfer pathways, such as espionage, the import of artifacts without concomitant knowledge, or siphoning of information or technologies from foreign direct investment, are even less likely than direct assistance to rapidly result in sudden innovations that threaten strategic stability. Nonetheless, they will in many cases result in some evolution, even if slow.

The effects of evolutionary or revolutionary advances in a country's forces on strategic stability is far from certain, and will depend on the co-evolution of other actors, timing, and the technologies involved. Strategic stability is inherently a relational concept: broadly speaking, it is the combination of crisis, first strike, and arms race stability in which no party has or perceives an incentive to change its force posture out of concern that a competitor might gain an advantage by using strategic weapons first in a crisis.[19]

In calculating strategic stability, it is insufficient to consider only a competitor's potential advances; it must also be compared to the advances of the United States and its allies and partners. Given the rate of technological change in U.S. armed forces today and the time it will take competitors to adopt and integrate inventions, even rapid diffusion may result in a competitor being years behind, having copied an old and consequently obsolete version of a given invention. Not all technology diffusion is likely to decrease strategic stability; the nature of the diffused inventions and how and whether they are adopted are likely to be important factors in whether strategic stability is increased or decreased. For example, if the technologies are integrated into a defensive or deterrent posture, they should increase stability.[20] A recent special issue on emerging technologies and strategic stability found varied implications across technologies (hypersonic glide vehicles, lethal autonomous weapon systems, and 3D-printing), system structures (centralized or decentralized), scaling of investment, and time (before or intra-war).[21]

[18] Montgomery 2013.
[19] Generalized from Acton 2013, 128. See Schelling 1960, chap. 9 for the classical formulation, and Colby and Gerson 2013 for a variety of interpretations.
[20] Jervis 1978.
[21] Garfinkel and Dafoe 2019; Horowitz 2019; Schneider 2019; Sechser, Narang, and Talmadge 2019; Talmadge 2019; Volpe 2019; Williams 2019.

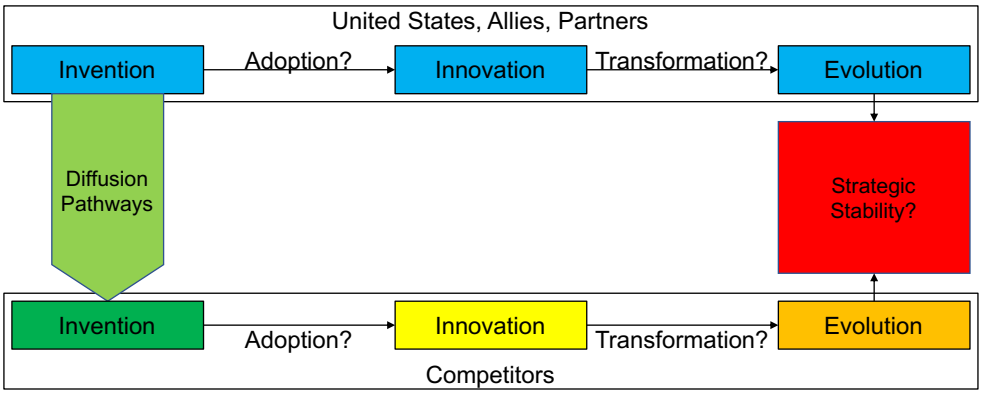

Figure 1: Invention, Diffusion, Innovation, Evolution, and Strategic Stability

This co-evolutionary process is modeled in Figure 1. The model starts with U.S., allied, or partner inventions in the top-left corner. The paper proceeds following this figure, first identifying relevant enabling inventions that, if diffused to competitors, could potentially disrupt strategic stability. These inventions include the enabling technologies underlying current attempts to transform U.S. force posture. It then discusses diffusion pathways and the potential for innovation through successful adoption of those inventions by competitors. It next evaluates the barriers for innovations to transform existing military systems, altering the evolutionary trajectory of their armed forces. Finally, it considers the net effects of that evolution on strategic stability through the examples of additive manufacturing and autonomy. It closes with a discussion of policy recommendations.

Invention

Starting with the top-left corner of Figure 1: the enabling inventions that the United States, allies, and partners are currently seeking to incorporate into innovations are the most salient risk of diffusion. As the system leader in technological development of military systems, the United States will be mimicked by peer and near-peer competitors because new technologies and forms created by the leading state are perceived as legitimate and modern,[22] or both. States that cannot compete in this way are likely to adopt asymmetrical strategies instead; however, smaller powers that pursue technologies in this way are unlikely to disrupt overall strategic stability simply due to their lack of overall power and the likely defensive or deterrent posture of such strategies (e.g., Anti-Access/Area Denial). This pattern will probably persist, as the United States follows a deliberate strategy of attempting to maintain or extend a significant technological advantage: what began in the 1950s as an "offset" to counter conventional superiority is now an attempt to sustain and advance military dominance through technological superiority. The directions of advanced research currently being pursued by the U.S. Department of Defense (DOD) consequently constitute an important (if potentially incomplete) set of candidate technological inventions for diffusion.

[22] Demchak 2003, 308.

Inventions in the Third Offset Strategy. Since World War II, the United States has consistently pursued new technologies to "offset" competitor numerical advantages. There have been two prior "offsets" in the post-World War II context: the "First Offset" that countered Soviet conventional superiority in Eastern Europe with a large and diverse nuclear arsenal, and the "Second Offset" once nuclear superiority was no longer guaranteed, which combined precision-guided munitions with superior command, control, and communications (and, more broadly, computers, intelligence, surveillance, and reconnaissance: together, C4ISR). Nuclear weapons modernization, diffusion of increasingly sophisticated C4ISR to competitors, and the rise of Anti Access/Area Denial strategies connected to a variety of weapons (anti-ship, anti-air, long-range strike, and anti-satellite) have chipped away at both offsets.[23] In response, the U.S. DOD has been taking a shotgun approach to creating a "Third Offset,"[24] investigating a variety of technologies including artificial intelligence, autonomy, cybersecurity, human systems, and space through partnerships with the private sector cultivated by new DOD initiatives, such as the Defense Innovation Unit (DIU).[25] This effort is inherently connected to dual-use technologies, since it specifically leverages links with innovative civilian enterprises rather than relying exclusively on military suppliers.

Technologies from the Civilian Sector. The technologies underlying the "Third Offset" are, by and large, the same enabling dual-use digital technologies that are prime candidates for diffusion and disruption absent efforts to limit their spread: machine learning, digitized manufacturing (including older CNC technologies as well as newer 3D printing ones), and technologies that underlie advanced sensors and communications. The primary role of enabling technologies in military innovation and diffusion is not surprising. Enabling technologies were foundational to many of the military-technical advances in the last century, and defense-related research, development, and procurement were key drivers of advancing these technologies.[26] In the present, the civilian sector is driving both creation and digitization of these enabling technologies, which makes them both inherently dual-use and more likely to diffuse.

The military is seeking to capitalize on these civilian-led technologies by bundling them together to transform military forces. For example, autonomy encompasses a bundle of artificial intelligence, advanced sensors, communications, and mobility. Digitized manufacturing can support practically any military technology that requires precision manufacturing, and is already being used in military aerospace applications.[27] Technologies developed by the civilian sector can be critical drivers for military interest, particularly in the area of autonomy, due to the extensive research and development in machine learning being carried out in that sector.[28] Indeed, assistance from the civilian sector may be crucial in this area; the United States is thought to be behind China with respect to three of the four "horsemen" of AI conflict—scale,

[23] Work 2015.
[24] Although the "Third Offset" nomenclature is not currently used, DOD is pursuing the same set of potential innovations in the same offices, although said offices are now less proximate to the Secretary. Whether this will lead to more or less productivity is debated.
[25] Defense Innovation Unit 2018.
[26] Ruttan 2006
[27] Volpe 2019, 815
[28] UNIDIR 2014.

foreknowledge, and strategic coherence—and only ahead on speed.[29] Even technologies related to the Third Offset that are not largely digital in nature are dual-use and frequently dominated by the commercial sector, underpinned by digital technologies, or both. For example, DIU's space portfolio is specifically meant to "access and leverage the growing commercial investment in new space," and human systems involving augmented reality and advanced communications. [30] Finally, cyber is both a set of technologies that can and have diffused to state and private actors *and* a major vector for diffusion of other digital technologies itself.

The United States does not have a monopoly on civilian invention, and so is hardly the only dual-use source of diffusion. For example, while the United States has relied heavily on the military for creation of new technologies, the German national model of development relies heavily on the civilian sector. While invention is a particular strength of the United States, taking inventions and adopting them by integrating them into existing systems in a way that leads to innovation and therefore significant military improvements is a difficult task. Germany is better at adapting inventions to particular industrial needs and diffusing them throughout particular sectors,[31] making it the second-most innovative country in the 2019 Bloomberg Innovation Index.[32] It is a leader in many dual-use-relevant areas, including in particular additive manufacturing, where it has become a leading developer.[33] This is in part due to the dense connections between government, industry, and universities, forming a "Triple Helix" that is well-suited to knowledge-intensive products and processes that are all destined for the open market—one of the primary pathways through which diffusion occurs.[34]

Diffusion

There are many different conduits through which inventions can diffuse to other states; this paper develops a four-fold typology, derived from whether the recipient receives the inventions via market exploitation (buy), direct assistance (beg), different forms of espionage (steal), or capability demonstration (copy). While diffusion or proliferation[35] in the broadest sense of "spread" can be conceptualized to include entirely indigenous development without technology transfer such as the French nuclear weapons program,[36] unassisted development is still subject to the barriers to invention, innovation, and evolution described in later sections, and strategies that seek to inhibit these processes and maintain strategic stability are still applicable.

[29] Demchak 2018
[30] Defense Innovation Unit 2018, 3.
[31] Breznitz 2014.
[32] Jamrisko, Miller, and Lu 2019.
[33] Office of Technology Assessment at the German Bundestag 2017, 2.
[34] Etzkowitz and Leydesdorff 2000.
[35] Diffusion (spread) and horizontal proliferation (an increase in the numbers of actors possessing something) are synonymous when discussing the diffusion of technology to additional actors; I use diffusion to refer to general technologies, and proliferation to refer to nuclear technologies as per conventional use in those domains.
[36] Scheinman 1965.

Buy: Market Exploitation. The strategy of leveraging civilian suppliers to obtain sensitive technologies inherently raises the likelihood of diffusion by creating a civilian marketplace for specific military demands. This tactic has been used numerous times for nuclear technologies (and their subsequent diffusion). The international supplier network created by Pakistan's nuclear weapons project, for example, made it easy to add new customers to the network once A.Q. Khan decided to deliberately assist other states with their nuclear weapons programs.[37] The diffusion of precision manufacturing meant that Khan's team could order the same centrifuge casings they used from a supplier in Malaysia to send to Libya for the development of its nuclear program. [38] However, this outsourcing to Malaysia was possible in part because the parts were relatively simple: manufacturing requirements for the centrifuge casings are much lower than those for the key internal components for the centrifuges. Nonetheless, the lower the unit costs and the greater commercial demand, the more likely is diffusion to occur.[39] Unit costs are likely to plummet for dual-use technologies, particularly those that are based on enabling technologies, for two reasons. First, enabling technologies tend to accelerate innovation, either improving product quality, decreasing unit costs, or both. Second, the protean nature of enabling technologies means that they are more likely to be incorporated across a wide variety of sectors, further increasing incentives to decrease the base cost of the underlying enabling technologies.[40]

Long supply chains can aid diffusion of information and allow recipients to better mask illegal procurement. Information on countries' defense priorities is revealed through open-market procurement contracts. Indeed, India's attempt to outsource parts of its overt centrifuge program inadvertently leaked not only their strategic priorities but also important technical knowledge regarding technical specifications of centrifuge components and related equipment. Similarly, the complexity of international supply chains created by open markets makes it easy to hide illicit procurement by importing controlled items into third countries such as India (among many other states with poorly implemented export controls) and then re-exporting them.[41]

Gaps between domestic supply and demand can also incentivize private actors to export technologies despite potential dual use. For example, Germany may be ahead of the United States in innovation, but is thought to be behind the United States in end uses of AM,[42] leaving German AM companies with fewer incentives to extensively investigate foreign buyers. Germany leans heavily on principles of open markets for both its export-driven economy and internal procurement needs. Markets also incentivize export of knowledge by private individuals. This is a hazardous loophole that was used by Khan, who recruited and paid Swiss, British, and German nationals to arrange for manufacturing and shipment of centrifuge parts for Libyan procurement.[43] These incentives are yet another potential vulnerability for export-control regimes.

---

[37] Khan 2012.
[38] Albright and Hinderstein 2004
[39] Horowitz 2010.
[40] Bresnahan and Trajtenberg 1995.
[41] Albright and Basu 2006.
[42] Office of Technology Assessment at the German Bundestag 2017, 1.
[43] Albright and Hinderstein 2004.

Another market mechanism for diffusion is through foreign direct investment (FDI). Diffusion through FDI is facilitated when firms are encouraged to invest in a recipient state. China's rules on foreign ownership and requirements to partner with local companies are designed to encourage FDI and capture as much knowledge and technology as possible:[44] FDI flows into China peaked at $139 billion USD in 2018.[45] In the opposite direction, recipient states can invest in companies abroad that produce defense-relevant technologies either directly or through state-controlled or influenced firms. Domestic attempts to reduce this pipeline may just lead recipient countries to locate suppliers in other states: changes in U.S. regulation led to a dramatic drop in Chinese investment in U.S. companies in 2018, while investment in Europe was fairly stable, and flows into Canada increased dramatically.[46] While sensitive acquisitions, such as the German robotics firm Kuka by the Chinese company Midea, now require state-level approval,[47] this is often delegated to market regulators whose chief remit is competition rather than diffusion of dual-use technologies. Many countries, including Germany, would admit that they are behind in overseeing and regulating these transactions.

Beg: Direct Assistance. Direct government-to-government assistance—whether through foreign military sales or transfers of dual-use or sensitive expertise, materials, or technology—is a primary conduit for diffusion. In the nuclear realm, this kind of "assistance" historically has been surprisingly frequent despite clear incentives for governments to keep the nuclear club small. Assistance with "sensitive" technologies, including uranium enrichment and plutonium reprocessing, has occurred at least 14 times between 1958 and 2002 according to one dataset (see Figure 2).[48] This does not count significant transfers of knowledge between the UK and the US, nuclear reactors with clear military purposes (North Korea to Syria), or less substantial cooperation such as a small research reactor from China to Algeria or uranium oxide and tritium trade between Israel and South Africa.[49]

An important aspect of Figure 2 is that it demonstrates both the diffusion of two dual-use inventions—and the limits of the effects caused by that diffusion. The reportedly successful cases (China, Pakistan, Israel, North Korea) are mixed in with a large number of cases of diffusion in which those inventions were never properly adopted (Libya, Iraq, Egypt)—or, in some cases, were adopted but failed to be transformed into a successful nuclear weapons program (Algeria, Iran, Japan, Brazil, Taiwan). It also draws attention away from successful cases of nuclear acquisition that did not benefit from this particular type of assistance (United States, Soviet Union, France, South Africa, India). The causes for failed adoption range from regime type to lack of oversight to normative influence, some of which are detailed below.[50] Note also that the motives for assistance varied as well: for example, while security motives (China–Pakistan) or trade in technologies (Pakistan–North Korea) were clearly present in some cases, others were sub-state actors driven by the invisible hand (Pakistan–Libya).[51] Figure 2 also

[44] Gilli and Gilli 2019
[45] Xinhua 2019
[46] Baker McKenzie 2019
[47] Reuters News 2016
[48] Kroenig 2010.
[49] On US–UK, see Gowing 1964, 1974a, 1974b; on North Korea–Syria, see Kerr, Hildreth, and Nikitin 2016; on China–Algeria, see Albright and Hinderstein 2001; on South Africa–Israel, see Liberman 2004.
[50] Braut-Hegghammer 2016; Hymans 2012; Montgomery 2013; Rublee 2009.
[51] Khan 2012.

demonstrates another aspect of nuclear weapons materials diffusion beyond the scope of this paper since it would require taking into account complex feedback loops among multiple actors simultaneously: secondary diffusion to additional actors. Encouragingly, only two of these transfers (Germany–Brazil, France–Egypt) originated in countries who were members of the Nuclear Suppliers Group at the time.

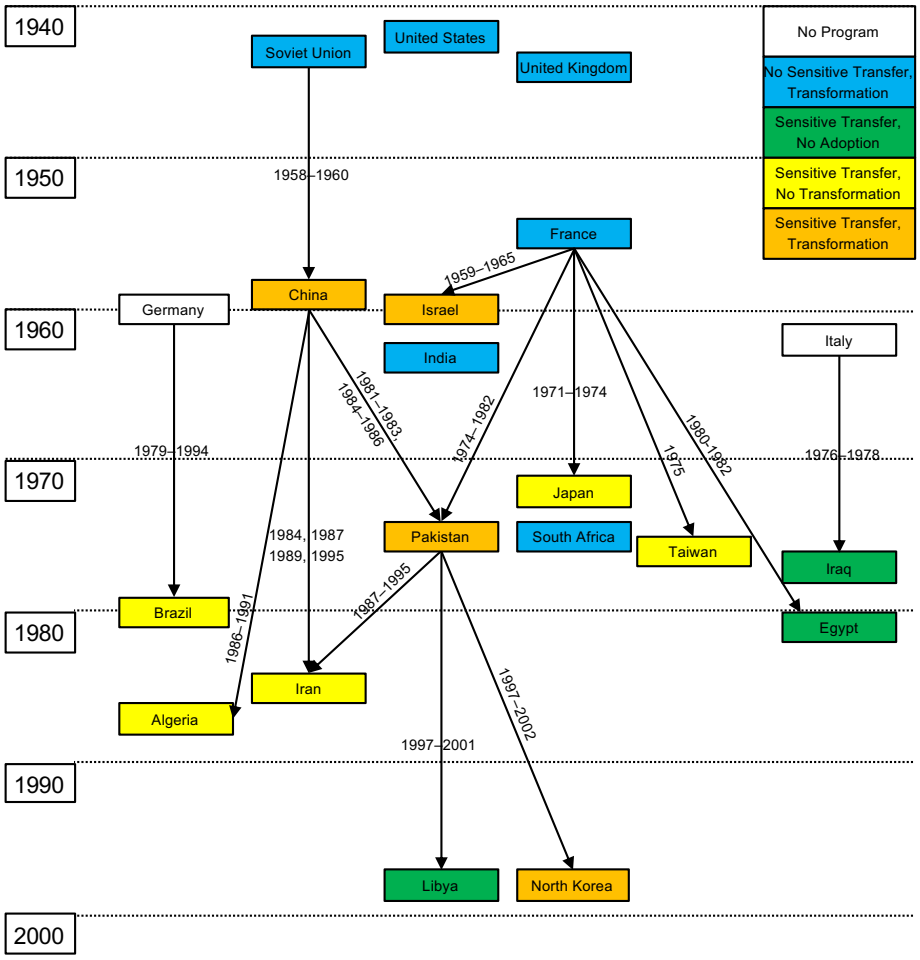

Figure 2: Technology adoption and transformation through deliberate transfer of sensitive nuclear technologies 1958–2002.[52]

[52] Sensitive technologies here are uranium enrichment and plutonium reprocessing. Height of top of node indicates year of transfer for recipients, first year of weapons pursuit (Bleek 2010) for countries that did not receive transfers, and first year as a nuclear-capable supplier (Fuhrmann 2009, 193) for countries that did not pursue nuclear weapons. Transfer data from Kroenig 2010.

Steal: Espionage. Espionage is another conduit for diffusion. Some accounts of nuclear proliferation argue that spying was crucial for the acquisition of both atomic and thermonuclear weapons by the Soviet Union and China, among other countries.[53] However, in-depth studies of both cases indicate that while espionage may have helped to a limited extent, the partial nature of the plans and ideas obtained and how they were used meant that they played a relatively minor role in the initial development of their nuclear weapons programs.[54] For example, the Soviet designers were only privy to partial information during the early design phase, and did not know they were producing a copy of the American design. [55] The leaders of the Soviet project (Beria and Kurchatov) withheld the U.S. plans and primarily used them to check the designers' work.[56] All of the stolen information was suspect, and had to be analyzed, deconstructed, and reverified. It is unclear that espionage ultimately saved the Soviets time, but it is apparent that it led to some inferior choices, including replacement of centrifuges with inefficient electromagnetic separation.[57] The main impediment to Soviet bomb development, in the end, was not the design, but rather the availability of uranium.[58]

The effects of espionage on the overall trajectory of the Soviet program is mixed. The decision to employ a U.S.-style weapon delayed the development and testing of their (much better) design and thus slowed down overall Soviet nuclear weapons development. Yet the choice to withhold information from the designers may have been a benefit in the longer term, since the Soviet physicists had to indigenously generate crucial tacit knowledge.[59]

Nonetheless, ongoing development and refinement of weapons designs has been assisted by continuing espionage: the Chinese theft of the W-88, the most advanced warhead in the U.S. arsenal,[60] could have helped with miniaturization of China's own arsenal. Ironically, additional cumbersome and largely symbolic security measures that choked off any supply of information, which were added after Wen Ho Lee[61] was falsely accused of leaking weapons designs, probably did more to stall innovation at Los Alamos than stymie innovation in other countries. Knowledge is a much more valuable diffusion product than information; focusing on preventing the corruption of or access to individuals with expert knowledge is probably the best export control of all.[62] With the free flow of information, preventing experts from traveling is insufficient: China hired a designer of the B-2 bomber to work remotely on a stealthy exhaust system for its cruise missiles.[63]

---

[53] Reed and Stillman 2009.
[54] See Gordin 2009; Holloway 1996; Lewis and Xue 1988 for evidence that it was relatively minor in the Soviet and Chinese cases.
[55] Holloway 1996, 138.
[56] Gordin 2009, 155.
[57] Gordin 2009, 152–53.
[58] Holloway 1996, 223.
[59] MacKenzie and Spinardi 1995.
[60] Wise 2011.
[61] Gusterson 2011.
[62] Ouagrham-Gormley 2014.
[63] Wise 2011.

However, the gold standard for diffusion is transfer of both technology and knowledge—having a group of experts with diverse backgrounds visit a recipient state with the relevant technologies to directly mentor their counterparts. This is very difficult without explicit state acquiescence. French assistance to Israel, for example, was originally designed to include all of the technological components required for a plutonium-based nuclear program,[64] and included visits by French engineers, who were "really top grade engineers who knew how to handle large-scale projects."[65] The project involved "hundreds" of French employees.[66] The Israelis did struggle to replace the large-scale assistance provided by Saint Gobain after the French terminated most assistance, eventually taking over construction of the most sensitive elements themselves.[67] Espionage cannot transfer invaluable tacit knowledge, and so will always fall short of this gold standard.

Large firms such as Saint Gobain can potentially provide entire systems and transfer the tacit knowledge needed to understand and run them effectively, making them attractive targets. However, the larger the firm providing technical assistance for sensitive projects, the more likely it is that they will have dedicated staff to engage in export controls and ensure propriety. Modern proliferators thus target small companies or individuals who may lack knowledge of export regulations (or be paid to not care). While this is not as effective as having diverse teams visit target states and try to pass on the necessary tacit knowledge, these kinds of scenarios are more effective in facilitating diffusion than acquiring artifacts or blueprints. And it is more difficult to prevent information, whether inside someone's head or in digital form, than specific pieces of technology from leaving the country even though both are equally "exports."

With the digitization of many of these technologies, cyber espionage has become an even more important path through which inventions can be stolen. Both the speed and the volume of exfiltration of sensitive information have increased dramatically. One account estimates the amount of data stolen by China from the United States alone to be around 50 terabytes. Ironically, the estimate itself was leaked by Edward Snowden.[68] According to one open-source account, China is thought to have obtained information on a number of important platforms from cyber exploits (F-22, F-35, Littoral Combat Ship, and RQ-4 Global Hawk).[69] These attacks targeted the U.S. DOD as well as key defense manufacturers (Lockheed Martin, Northrup Grumman, and Raytheon). Nonetheless, cyber espionage tends to supplement foreign technology acquisitions, traditional espionage, and indigenous R&D rather than serve as a primary driver of Chinese military modernization.[70] Despite these leaks from established military contractors, the European Union and the United States are both expanding the number of defense contractors and including companies that have traditionally been in the civilian sector. This has the unintended effect of producing a target-rich environment for cyber espionage.

[64] Cohen 2010, 57.
[65] Cohen 1998, 68
[66] Cohen 1998, 71
[67] Cohen 1998, 75
[68] Gady 2015.
[69] Long 2015, 106–9.
[70] Long 2015, 113.

Copy: Demonstrating Capabilities. Finally, some diffusion results simply from capability demonstration: the most important information about some inventions is that they are possible rather than the specific details as to how they work. Nuclear weapons are a prime example of this: the biggest initial secret was that first atomic (via implosion) and later thermonuclear weapons would actually work in practice. More recently, once the United States developed (and then demonstrated) stealth technologies in the form of the F-117 during the Persian Gulf war, both Russia and China were inspired to make major investments both in stealth technologies and in counter-stealth sensing[71]—and, of course, in espionage.

From Diffusion to Evolution

Regardless of the path by which technological inventions are initially acquired, there is still a long road an actor must take before those inventions can make a tangible difference in the balance of forces. A series of barriers (some dependent on the technology in question) can impede and slow adoption, innovation, or both.

From Diffusion to Innovation: Barriers to Adoption. Whether a given technological invention is purchased, stolen, or donated, it still must be adopted successfully in order to have a chance at producing significant effects. All forms of diffusion typically require the ability to produce technologies. Without the ability to manufacture a technology indigenously, actors are either dependent on foreign suppliers—making efforts to impede adoption such as sabotage possible—or must make do with whatever limited set of samples they have already acquired. In either case, this makes transformation unlikely due to an inability to implement the technology on a system-wide basis.

North Korea follows an explicit import-then-indigenize strategy for much of its nuclear enterprise, from centrifuges to produce highly enriched uranium to the specialized vehicles used to transport and erect its ballistic missiles. This strategy is complemented by North Korea's extensive smuggling network, developed and refined over decades of isolation.[72] North Korea does not simply reverse engineer technologies to produce copies of imports: extensive modification and innovation are hallmarks of their process. They seek to indigenize both design and production of the imports. This allows them to generate the tacit knowledge required to build and operate these systems, although not without difficulty.[73] Indeed, it is the approach to adoption and transformation that seems to determine the pace of advance rather than the method of acquisition of an invention. Approaches that rely on manufacturing from abroad cannot generate this tacit knowledge.[74]

The North Korean strategy can be compared with Iranian and Libyan approaches. Iran based their main centrifuge production for years on an inferior import from Pakistan (the P-1) before doing their own experimentation and innovation. Libya hardly got past uncrating a few parts sent

[71] Pietrucha 2016
[72] Chestnut 2007.
[73] Pollack 2017.
[74] Montgomery 2013.

from Pakistan. This is in large part due to a gap between domestic absorption capacity and the demands of the technology.[75] Absorption capacity (also referred to as adoption capacity or enterprise capacity) includes all of the organizational factors needed to successfully adopt an invention: financial ability; organizational capital;[76] and a sufficient educational, technological, and industrial base.

The indigenization of sophisticated military hardware is much more difficult now than it was in the age of the battleship. This is due to the vastly increased complexity of military technology, its tight integration with organizational practices, and very high tacit knowledge requirements. These all set much higher barriers to adoption than older technologies created during, e.g., the Industrial Revolution. China's program to replicate the F-22 has benefited from peerless cyber espionage efforts, direct assistance from Russia and Israel, foreign direct investment that imported significant knowledge, and samples of fighters that they could reverse engineer. Yet they have struggled, producing a fighter (the J-20) with inferior stealth capabilities, engine performance, and avionics.[77] Nuclear weapons similarly have a high tacit knowledge requirement, which significantly limits the effectiveness of diffusion.[78]

Finally, modern military technologies are deeply embedded within a set of complex organizational practices, and so are difficult to diffuse to different contexts. The F-35, for example, is designed to be connected with a variety of other U.S. systems, sharing sensor data on targets, mission, and aircraft status with other strike aircraft and operation centers on air, sea, and land. To fully adopt the F-35 requires embracing a set of other systems, a high barrier even for technologically sophisticated allies and partners. The F-35 also requires a commitment to *not* connect it to other systems (hence the denial of the F-35 to Turkey in the wake of its acquisition of a Russia S-400 air defense system). Indeed, the platform continues to have adoption issues,[79] including the inability of F-22s to send information to the F-35. [80]

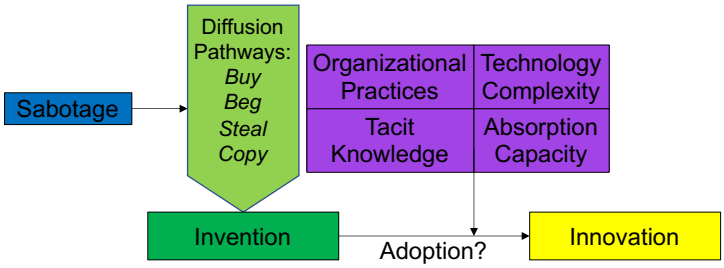

Figure 3: Barriers to Adoption

In sum, there are a number of likely barriers to adoption of diffused technologies (See Figure 3). Even prior to adoption, actors are frequently reliant on foreign suppliers before indigenization, creating new indicators and warnings and making actors vulnerable to sabotage. Between

[75] Montgomery and Volpe 2017.
[76] Horowitz 2010, 30–39. Horowitz includes critical task focus, experimentation, and organizational age under organizational capacity.
[77] Gilli and Gilli 2019.
[78] Dennis 2013; MacKenzie and Spinardi 1995; Montgomery 2005.
[79] Insinna 2019.
[80] Bloomberg 2018.

invention and innovation, four additional barriers await: the complexity of the technologies make them resistant to adoption; a lack of absorption capacity can hinder adoption; and the re-creation of requisite tacit knowledge and associated organizational practices is difficult.

Innovation to Evolution: Barriers to Transformation. The threat posed by the diffusion and adoption of technologies depends, in large part, on the nature of the changes caused by acquisition. Typically, technological innovations are assumed to have at least evolutionary and possibly revolutionary effects on a competitor's capabilities. Evolutionary effects tend to accelerate existing development trajectories, while revolutionary ones result in fundamental changes to those trajectories, potentially enabling leap-frogging and strategic surprise. However, it is also possible to have a null or even devolutionary effect if the technologies acquired are a poor fit for the country by wasting resources or revealing intentions, producing blowback.[81] Alternatively, if the military fails to properly integrate innovations, it may result in stasis rather than transformation.

Military revolutions are the most potentially dangerous to strategic stability; fortunately, they present a particularly high bar for any actor to jump over. The canonical definition of a military revolution is "the application of new technologies into a significant number of military systems combine[d] with innovative operational concepts and organizational adaptation in a way that fundamentally alters the character and conduct of conflict."[82] Note that this definition includes four separate processes which need to occur for a revolution to result in a leap forward for military effectiveness: technological change, systems development, operational innovation, and organizational adaptation. Unless new technologies are built into systems (or systems are rebuilt around technologies), operations are altered to take advantage of them, and organizations persuaded to adopt them wholeheartedly, revolutions cannot be fully (or maybe even partially) realized. There is some debate over whether the military-technical revolution associated with the second offset is or even can be fully implemented.[83] For example, it is unclear whether the United States can successfully and completely implement certain aspects of networked warfare without also adopting high-reliability practices.[84] Absent such practices, complex, large-scale military systems can lead to catastrophic failures, killing soldiers, civilians, or both.[85] This is one of the most important concerns about adoption of autonomous weapons.[86]

Thus, even if an invention is successfully acquired and domestic production (or reliable foreign production) of its constituent parts is ensured, significant hurdles to innovation remain. While innovation in any domain involves the proper adoption of technologies and integration into systems, military innovation has additional barriers: it must change the manner in which military formations function in the field, be significant in scope and impact, and be equated with greater military effectiveness.[87] Military organizations are notoriously resistant to innovation, typically

[81] Montgomery and Volpe 2017.
[82] Krepinevich 1994, 30.
[83] Krepinevich 2002.
[84] Demchak 1996.
[85] Rochlin 1991, 1998.
[86] Carvin 2017.
[87] Grissom 2006, 907.

requiring some kind of competitive motivation or resource threat to change.[88] Change can occur due to civilians asserting control over a recalcitrant military; competition over resources between services; competition within a given service over theories of victory; and altering organizational culture (which can be shaped internally, from external shocks, or through foreign emulation) to promote change.[89] Note that much of the literature on military organizations tends to be based on the United States or European countries—for example, models of interservice competition tend to assume a U.S.-style distribution among services.

Some military innovations do come from bottom-up processes, where existing platforms are repurposed creatively by end users. These processes may also be an important factor: in circumstances where bureaucratic inertia stymies innovation, successful improvisation by combat units can produce change. Examples of this include repurposing anti-aircraft guns as anti-tank weapons in WWII[90] and the US Army Force XXI initiative, which digitized and decentralized command and control systems, allowing Iraq War combatants to operate more aggressively, particularly when dispersed. In the field, soldiers repurposed "email" and "chat room" functions as less-cumbersome communications and battle-tracking systems.[91] During the Gulf War, soldiers duct-taped Garmin GPS systems to their dashboards to navigate in the desert. These modern examples demonstrate how enabling technologies can spark innovation: the more use-cases a technology supports, the more likely that technology will be adopted and even possibly transform systems through decentralized experimentation rather than through central planning.

Militaries are resistant to transformation (whether top-down or bottom-up) by virtue of their internal organizational structures. Modern militaries, by the nature of the tasks they need to complete, are organized as large technical systems (LTS)— spatially extended and functionally integrated socio-technical networks.[92] This form of organization presents additional barriers related to the difficulty of successfully rewiring these networks to incorporate new innovations. The complexity of the systems that need to be transformed to take full advantage of an innovation requires a great deal of local knowledge and expertise to maintain properly, much less change. Added to this problem is the fact that innovations are exceedingly difficult to re-create since they must conform to a system's "technological style"—"the widely varying shape `one and the same' technology takes under different geographical, political, legal, and historical conditions."[93] A considerable amount of adaptation is always necessary, and without skilled, knowledgeable management, transformation is even more challenging.

Accordingly, failure to adopt or transform is often related to regime type—for example, neopatrimonial and personalistic regimes seem to pursue nuclear weapons at a greater rate but

[88] Posen 1984.
[89] Grissom 2006, 908–19.
[90] D'Este 1983, 375–79.
[91] Grissom 2006, 926–928.
[92] Mayntz and Hughes 1988, 5. A lengthier definition is also given in the introduction: "…systems of machineries and freestanding structures performing, more or less reliably and predictably, complex standardized operations by virtue of being integrated with other social processes, governed and legitimated by formal, knowledge-intensive, impersonal rationalities." Joerges 1988, 23–24.
[93] Joerges 1988, 12.

succeed less often due to poor governance. In rare cases (such as China and North Korea), they can succeed if actors succeed in insulating those enterprises from wider patterns of patrimonial/personalistic rule. For example, mismanagement by personalist regimes in Libya and Iraq doomed their nuclear programs (although Iraq did notably better).[94] Governments such as Ghaddafi's Libya and Peron's Argentina have been duped by domestic or international hucksters promising get-nukes-quick schemes due to a lack of scientific expertise or trust of their own scientists.[95]

Finally, states may adopt a technology (or set of technologies) but due to lack of sufficient strategic motivation may either put little effort into transforming military forces or may be satisfied with restricting innovation to the civilian sector as a hedge against future contingencies. Lack of motivation is inherently difficult to study, but appears to have been a significant influence in keeping a number of nuclear weapons programs at the exploration phase (Japan, Switzerland, Sweden, Australia, West Germany) or a limited pursuit phase (Brazil, Argentina) due to a lack of a clear motivation for continuing any further. South Africa developed weapons, but failed to integrate them into their military in any significant way. This failure can be attributed to a number of causes: the program was disconnected from the military due to it initially being a partial byproduct of mining,[96] and there was no clear strategic threat to which nuclear weapons were a solution. This lack of motivation and integration permitted the only extant case of nuclear rollback.[97]

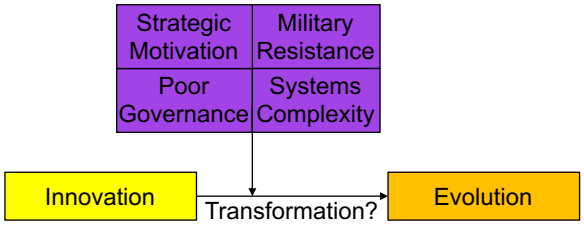

Figure 4: Barriers to Transformation

In sum, there are barriers to military systems transformation (see Figure 4) in addition to the barriers to diffusion and adoption previously discussed: a tendency of the military to resist innovations; the inherent complexity of the military systems that need to be transformed; various forms of poor governance that compound the inherent difficulties of transformation; and lack of strategic motivation.

[94] Braut-Hegghammer 2016.
[95] Hymans 2012; Montgomery 2013; Way and Weeks 2014.
[96] Flank 1993.
[97] de Villiers, Jardine, and Reiss 1993.

Enabling Technologies: Additive Manufacturing. Many of the above examples focused on inventions that constituted parts of entire weapons systems (predominantly nuclear weapons). Might the diffusion of enabling technologies from the civilian sector follow a different trajectory or result in strategic surprise? Additive manufacturing demonstrates many of the steps in this overall invention-to-evolution process, as well as many of the pitfalls. Enthusiasts and doomsayers alike see AM as a technology that will quickly diffuse, revolutionizing manufacturing of everything from conventional weapons to nuclear weapons, writing articles with titles such as "You can print your own guns at home. Next it will be nuclear weapons. Really."[98] Although this is highly unlikely (as discussed below), it is notable that this technology has been used for a number of military applications already: "General Electric, Aerojet Rocketdyne, and the Chinese People's Liberation Army are already using AM to print sophisticated metal parts for jet engines, rocket propulsion systems, and fighter aircraft, respectively."[99]

However, as one assessment put it, "ideas regarding the performance, potential applications and impacts of AM technologies are manifold and often highly exaggerated." The adoption of AM presents difficulties due to problems constructing larger components, low build-up rates, manual upstream and downstream production steps, and lack of knowledge of the properties of printed components compared to traditionally machined ones.[100] The latter may be more of a disadvantage for risk-averse enterprises seeking to replace existing processes than for risk-acceptant competitors looking to get ahead: just a few years ago, Los Alamos National Laboratory had (finally) concluded that uranium pits could be manufactured using direct casting instead of wrought casting,[101] and was still using a sixty-year-old machine for measuring the symmetry of pits.[102] Ironically, additive manufacturing may offer a way of replacing parts for these ancient machines even if it doesn't offer a replacement solution. This particularly cautious approach is driven partially by the absence of full-systems testing since 1992 and the collapse of the U.S. nuclear weapons manufacturing complex. Similarly, the traditional conservativism of most militaries is also likely to prevent adoption of significant innovations like additive manufacturing from doing more than improve efficiency at the margin—with the possible exception of the most risk-acceptant actors.

Could additive manufacturing be the kind of enabling technology that leads to strategic instability? It is likely to be very disruptive for traditional manufacturing and will certainly have a large, short-term effect on small arms and light weapons proliferation. Yet, the sheer volume of contemporary competitive manufacturing, the lengthy duration over which stockpiles have been built up, and the abundant trade of small arms has resulted in a world already awash with such weapons. The availability of small arms dwarfs the availability of the set of materials that would be required to print even simple small arms. Moreover, simple plastic 3D-printed gun designs are just a structure that requires the addition of firing pins and other metal parts to properly work—and, of course, ammunition. While the ability to print incredibly simple weapons such as grenade

[98] Tirone and Gilley 2015.
[99] Kroenig and Volpe 2015, 7.
[100] Office of Technology Assessment at the German Bundestag 2017, 1.
[101] Korzekwa 2012, 19.
[102] Putnam 2012, 28.

launchers is useful for rapid prototyping or even eventual manufacture,[103] the myriad inputs required will encourage at least somewhat centralized manufacturing rather than a scenario in which an actor of concern will hide "in a jungle" and "produce a cache of weapons outside the reach of a state or other regulatory body."[104] Creative employment of additive manufacturing—like the re-employment of anti-aircraft weapons, GPS receivers, or email systems—may lead to innovation. However, the scale of such innovations is likely to be small and rarely superior to traditional methods of acquiring light arms, and so is unlikely to cause significant shifts in the balance of forces.

The proliferation of weapons of mass destruction and the means of delivering them has also been a major concern of AM assessments. Innovations in AM that affect WMD proliferation could disrupt strategic stability either through arms racing due to rapid manufacturing or through proliferation to additional actors by facilitating stealthy production. Arms racing is certainly a possibility, although it would almost certainly require testing even if the hurdles to printing fissile materials were to be overcome. Proliferation presents a more complex case, since AM may make it easier for facilities to be hidden (since eliminating waste streams removes a significant source of indicators and warnings) and for proliferators to circumvent sanctions.[105] Additionally, AM may lower the barriers to entry, or accelerate and augment traditional development pathways.[106]

However, the indicators and warnings problem due to the lack of waste streams mainly applies to actual pit production (or a few other easily-detectable elements). A building full of 3D-printed centrifuges will give off as much heat as a building full of conventionally-manufactured ones. Even with the relative stealth of centrifuge programs,[107] facilities can be located through open-source methods due to advances in sensing technologies and the ability to crowdsource intelligence collection.[108] It may also provide for new indicators and warnings: unless key materials can be indigenized, orders of certain powders such as maraging steel will provide warnings where orders of (some) aluminum tubes did in the past.[109] While printing of weapons-grade materials into the core for a nuclear weapon is clearly out of reach for the present,[110] some of the components of systems that produce fissile materials could be made using additive manufacturing. While the build files for these components are digital and consequently easier to spread and the machines are not (yet) export-controlled, the tacit knowledge and machinery

[103] Burns and Zunino 2017.
[104] Johnston, Smith, and Irwin 2018, 7
[105] Atherton 2018; Lucibella 2015.
[106] Volpe 2019, 820.
[107] Kemp 2014.
[108] Hanham et al. 2017; Panda 2018.
[109] The North Korean apparent order of aluminum tubes for their P-2-based centrifuges turned out to be a good indicator—samples they gave the U.S. government had highly enriched uranium on them: see Hecker 2008, 46–47. The Iraqi order of aluminum tubes that were actually for rocket motors was, well, not: see Albright 2003.
[110] Although our national labs have already indicated some success with reactive and radioactive powders, including a Uranium-Niobium alloy. See Marggraff 2015.

requirements for additive manufacturing are quite high,[111] and some of the powders required are already controlled.[112]

The list of countries that are actively generating expertise on additive manufacturing is an admixture of potential competitors who may wish to exploit them for the purposes of force transformation (China, Iran), emerging and regional powers (India, South Africa), and allies and partners (United States, Germany, Taiwan).[113] It is less apparent how advanced North Korea is, although they are clearly applying their usual practice of indigenization to the issue, albeit starting from a very simple base of copying an old model of MakerBot.[114] However, they quickly replaced the copy with an indigenized model a few months later. Nonetheless, North Korea already has a significant CNC manufacturing capability in place for its nuclear and missile programs—reverse engineered, naturally[115]—and so would benefit far less than a new proliferator would.

Additive manufacturing could, in fact, help to contribute to strategic stability—if strategies to clearly signal that a state is employing dual-use technologies for civilian purposes can be demonstrated. Signaling could occur through accepting an intrusive monitoring regime, allowing dependence on foreign suppliers, or employing third parties to underwrite nonproliferation commitments.[116] Additionally, it may allow advanced states with strong enterprise capacity to follow policies of restraint: the deterrence value of demonstrating a strong AM capacity while remaining a non-nuclear weapons state may be greater than the value of break-out.[117]

Enabling Technologies: Autonomy. While AM is likely to have effects only at the margin on strategic stability, other enabling technologies may have more significant effects. Unlike AM, exploring machine learning and the technologies that underpin advanced sensing and communications capabilities would be much too broad to come up with useful conclusions. However, autonomy (which combines together these technologies as well as others) provides a useful lens through which the relationship between strategic stability and these underlying enabling technologies can be explored.

Lethal Autonomous Weapons Systems (LAWS) are applications of autonomy that can affect strategic stability. A recent exploration of the potential relationship between the diffusion of LAWS and strategic stability raised significant concerns.[118] In particular, the potential for increased speed of operation and decreased human control were likely to create incentives to strike first, undermining both deterrence and crisis stability. Moreover, arms control is quite difficult, distinction strategies less possible, and arms racing more likely due to the difficulty of confirming that systems are (or are not) LAWS. Machine learning itself is often opaque and

[111] Christopher 2015, 21.
[112] Nelson 2015.
[113] Johnston, Smith, and Irwin 2018, 6.
[114] Asia Times 2017.
[115] Pollack 2017, A109.
[116] Volpe 2019, 825.
[117] Montgomery and Volpe 2017.
[118] Horowitz 2019.

difficult to "read out," further compounding the difficulty of understanding the nature of the highly complex neural networks that underlie decisions.

Fortunately, militaries are likely to be reticent to deploy truly autonomous systems. Military systems can be autonomous along four dimensions: trigger, targeting, navigation, and mobility. Systems that only exhibit three of these four characteristics (keeping humans "in the loop") have proven acceptable to the military.[119] Systems that exhibit every characteristic are unlikely to be approved by military organizations, due to their general conservativism, desire to maintain independence, and organizational culture. Computer vision and AI is still in its infancy,[120] and even very small false positive identification rates could have disastrous consequences, particularly away from conventional battlefields, which should reinforce the military's natural reticence to adopt such technologies.[121]

In addition to military resistance, other barriers to systems transformation will apply. Systems complexity is an inherent problem of autonomy. The more complex the machine learning, the more likely it is that an autonomous system will act unpredictably and cause accidents, whether due to deliberate spoofing or the fog of war. Nevertheless, like other enabling technologies, more risk acceptant actors may be willing to deploy these systems despite the risk of accidents in order to offset other actors' technological advantages. Russia and China have invested heavily in artificial intelligence, and Russia in particular is known to see it as a revolutionary technology that can offset other U.S. advantages. This makes arms control and dual-use distinction less plausible as strategies, and attempting to ban autonomous weapons entirely may give an advantage to actors who are more insulated from normative pressure.[122]

Recommendations

Putting together Figure 1, Figure 3, and Figure 4 and overlaying additional potential points of leverage to slow this process results in the complete model pictured in Figure 5. Despite the large number of barriers to adoption and transformation, it is still prudent to implement measures to prevent the diffusion of technologies, alter incentives for arms racing, and try to mitigate the security dilemma whether with dual-use or single-use technologies. As with countering weapons of mass destruction,[123] most of the opportunities for preserving strategic stability come from prevention of diffusion rather than from measures to contain technologies after diffusion. Since many technologies that diffuse will not be threats either because it will not lead to transformation or because the time lag will limit the instability caused by that transformation, policymakers must carefully weigh the likelihood of instability against the cost of preventing diffusion. Nonetheless, baking security features into technologies that could be harmful if diffused (i.e., security by design) will minimize future costs.

[119] Roff 2015.
[120] Karpathy 2012
[121] Robbins 2016
[122] Horowitz 2019.
[123] U.S. Department of Defense 2014

Simple measures such as implementing export controls on specialized additive manufacturing equipment that can be used to produce large, complex components that are crucial to certain proliferation pathways (AM powders are already regulated as dual-use) are relatively straightforward.[124] As one publication put it, "An approach to prevent a possible proliferation of armament technologies by means of AM technologies could consist in making the export of at least particularly powerful systems and associated materials subject to authorisation."[125] Decisions to restrict, however, must be made strategically—that is, taking into consideration alternate paths to diffusion that might be used instead by proliferators. If buying is not an option, can actors easily turn to other sellers or other pathways: begging, stealing, or copying? Will implementing export controls simply send signals that indicate that such equipment is strategically valuable and therefore desirable? Do exports produce strategic leverage in other ways through inducing dependence on supplies, discouraging domestic invention, innovation, and production, enabling monitoring, or opening opportunities for sabotage?[126]

Cyber security measures to mitigate the nearly constant stream of leaks and vulnerabilities are another straightforward measure; although organizational incentives push against effective cyber security, improvements are not hopeless.[127] The mere existence of the possibility of cyber or other forms of sabotage (discussed earlier) increases the cost of using stolen technologies. However, cyber sabotage can in practice be a double-edged sword, releasing code that can be repurposed for other uses. It may not even offer a very good value when considering the costs of attacking versus defending vis-à-vis some competitors.[128] Moreover, stockpiling key vulnerabilities means that friendly systems can be hacked by other actors if those vulnerabilities go undiscovered and unpatched.

Improved monitoring of end-use cases for legally exported dual-use enabling technologies would raise barriers to repurposing those technologies for military uses. The lowest-cost improvements in this area may lie in aiding countries that are capable of adopting recent enabling technologies but do not have strong export controls. Another relatively low-cost improvement for would be to realign the incentives built into regulatory systems to include national security as well as commerce to encourage businesses to comply with export controls. A recent World Bank Group publication, "Building and Sustaining National Educational Technology Agencies," listed a set of twelve lessons from cross-national experiences, none of which addressed export controls or other methods of preventing the proliferation of dual-use technologies for malignant purposes.[129] These can be relatively easily fixed.

[124] Nelson 2015.
[125] Office of Technology Assessment at the German Bundestag 2017, 4.
[126] I thank Richard Danzig for pointing out the need to consider the net effects of implementing such controls.
[127] Jones 2013.
[128] Slayton 2017
[129] Trucano and Dykes 2017, 2.

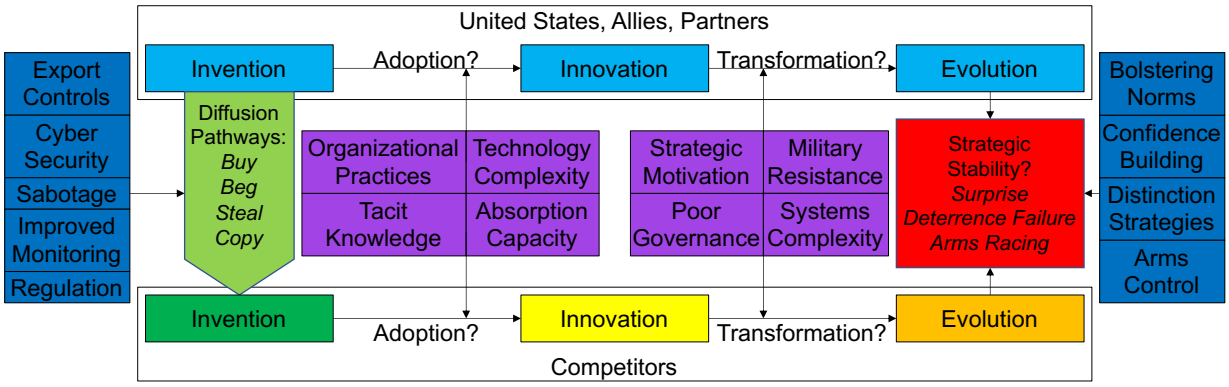

Figure 5: Responses to Invention, Diffusion, Innovation, Evolution, and Strategic Stability

Once technologies have diffused to the point where formerly rare inventions are commonplace, policy options are somewhat more limited. Many of the barriers to adoption and transformation are inherent to the technology, the recipient, or both. Strategic motivations, however, are malleable, whether through bolstering norms through existing treaties and moral suasion or through confidence-building measures and other signaling practices that can reduce the security dilemma. Distinction strategies may be possible for technologies that are relatively easy to monitor like additive manufacturing, allowing actors that wish to signal their benign intentions to do so. Arms control can be successful when use cases can be clearly and credibly communicated (like with some scenarios for additive manufacturing), but may be less successful when the technologies are more opaque (most applications of autonomy). Regardless, a shared perception of the threat posed by the diffusion of dual-use digital technologies to strategic stability is necessary for arms control measures to be implemented.

Digitized, dual-use enabling technologies, such as additive manufacturing, artificial intelligence, and the technologies underpinning advanced sensing and communication, are likely to diffuse. Fortunately, like single-use technologies, the more complex the end-use cases, the higher the barriers to adoption, transformation, and evolution, and the lower the likelihood of strategic instability. There are a number of low-hanging policy options to decrease the likelihood of diffusion, as well as some options to address the consequences of diffusion. It is important to note that some of the barriers identified here are extensions of existing efforts, and that the best strategy here may be to continue invention and innovation. These policy options before and after diffusion thus serve as additional hedges by limiting diffusion pathways (export controls, cyber security, sabotage, improved monitoring, regulation) and stabilizing outcomes (bolstering norms, confidence building, distinction strategies, arms control).

None of these recommendations should be taken to mean that efforts by the United States to adopt and transform its military will be benign or smooth. The barriers to adoption and transformation affect the United States, partners, and allies as much as they affect competitors. Indeed, the experience of the F-35 demonstrates that innovation is very difficult even given the best possible access to resources. Constantly seeking additional offsets without careful consideration of possible strategic diffusion and adoption by competitors can be counterproductive to security and strategic stability, promote arms racing, and alter strategic motivations for the worse. Moreover, some of these technologies may open up the possibility for dangerous or even catastrophic outcomes, such as the dramatically increased probability of

accidents inherent in complex autonomous systems. Caution and self-reflection regarding accidents, diffusion, and net effects on norms may be the most effective stabilizing strategies that the United States and its allies and partners can pursue.[130]

[130] Danzig 2018.

About the Author

Alexander H. Montgomery is an associate professor of Political Science at Reed College. He has a B.A. in Physics from the University of Chicago, an M.A. in Energy and Resources from the University of California, Berkeley, and an M.A. in Sociology and a Ph.D. in Political Science from Stanford University. He has been a Council on Foreign Relations International Affairs Fellow in Nuclear Security with a placement in the US Office of the Secretary of Defense (Policy) working for the Deputy Assistant Secretary of Defense for Countering Weapons of Mass Destruction. His portfolio included writing a new Department of Defense Strategy for Countering Weapons of Mass Destruction. He has been a joint International Security Program/Managing the Atom Project Research Fellow at the Belfer Center for Science and International Affairs, Kennedy School of Government, Harvard University; a post-doctoral fellow and a visiting assistant professor at the Center for International Security and Cooperation, Stanford University; and a residential fellow at the Woodrow Wilson International Center for Scholars. He has published articles on nuclear proliferation and on the effects of social networks of international organizations on interstate conflict, and is the co-editor of the *Oxford Handbook of Political Networks* (2017) with Jennifer Nicoll Victor and Mark Lubell.

Acknowledgements

I am grateful to Dr. Amy J. Nelson for providing extensive feedback on drafts and to Dr. Richard Danzig for comments.

Bibliography

Acton, James M. 2013. "Reclaiming Strategic Stability." In *Strategic Stability: Contending Interpretations:*, edited by Elbridge A. Colby and Michael S. Gerson, 117–46. Fort Belvoir, VA: Defense Technical Information Center. doi:10.21236/ADA572928.

Albright, David. 2003. *Iraq's Aluminum Tubes: Separating Fact from Fiction*. http://www.isis-online.org/publications/iraq/IraqAluminumTubes12-5-03.pdf.

Albright, David, and Susan Basu. 2006. "India's Gas Centrifuge Program: Stopping Illicit Procurement and the Leakage of Technical Centrifuge Know-How." http://www.isis-online.org/publications/southasia/indianprocurement.pdf.

Albright, David, and Corey Hinderstein. 2001. "Algeria: Big Deal in the Desert?" *Bulletin of the Atomic Scientists* 57 (3): 45–52. doi:10.2968/057003014.

———. 2004. "Libya's Gas Centrifuge Procurement: Much Remains Undiscovered." http://www.isis-online.org/publications/libya/cent_procure.html.

Asia Times. 2017. "Could Pyongyang's Nuke Missile Program Get 3D Printers?" August 17. https://cms.ati.ms/2017/08/pyongyangs-nuke-missile-program-may-get-3d-printers/.

Atherton, Kelsey. 2018. "In the Future, Iran Could 3D-Print Its Way around Sanctions." *C4ISRNET*. May 9. https://www.c4isrnet.com/it-networks/2018/05/09/in-the-future-iran-could-3d-print-its-way-around-sanctions/.

Baker McKenzie. 2019. "Chinese FDI into North America and Europe in 2018 Falls 73% to Six-Year Low of $30 Billion." January 14. https://www.bakermckenzie.com/en/newsroom/2019/01/chinese-fdi.

Bas, Muhammet A., and Andrew J. Coe. 2012. "Arms Diffusion and War." *Journal of Conflict Resolution* 56 (4): 651–74. doi:10.1177/0022002712445740.

Blackford, Jacob. 2005. "Multilateral Nuclear Export Controls After the A.Q. Khan Network." Institute for Science and International Security. http://www.isis-online.org/publications/expcontrol/multilateralexportcontrols.pdf.

Bleek, Philipp C. 2010. "Why Do States Proliferate? Quantitative Analysis of the Exploration, Pursuit, and Acquisition of Nuclear Weapons." In *Forecasting Nuclear Proliferation in the 21st Century: Volume 1, the Role of Theory*, edited by William C Potter and Gaukhar Mukhatzhanova, 159–92. Stanford, Calif: Stanford University Press.

Bloomberg. 2018. "Why America's Two Top Fighter Jets Can't Talk to Each Other." *Bloomberg.Com*, April 2. https://www.bloomberg.com/news/articles/2018-04-02/why-america-s-two-top-fighter-jets-can-t-talk-to-each-other.

Braut-Hegghammer, Malfrid. 2016. *Unclear Physics: Why Iraq and Libya Failed to Build Nuclear Weapons*. 1 edition. Ithaca: Cornell University Press.

Bresnahan, Timothy F., and M. Trajtenberg. 1995. "General Purpose Technologies 'Engines of Growth'?" *Journal of Econometrics* 65 (1): 83–108. doi:10.1016/0304-4076(94)01598-T.

Breznitz, Dan. 2014. "Why Germany Dominates the U.S. in Innovation." *Harvard Business Review*, May. https://hbr.org/2014/05/why-germany-dominates-the-u-s-in-innovation.

Burns, Seung kook "Sunny," and James Zunino. 2017. "RAMBO'S Premiere." *Army AL&T*, June, 67–73.

Carvin, Stephanie. 2017. "Normal Autonomous Accidents: What Happens When Killer Robots Fail?" SSRN Scholarly Paper ID 3161446. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3161446.

Chestnut, Sheena E. 2007. “Illicit Activity and Proliferation: North Korean Smuggling Networks.” *International Security* 32 (1): 80–111. doi:10.1162/isec.2007.32.1.80.
Christopher, Grant. 2015. “3-D Printing: A Challenge to Nuclear Export Controls.” *Strategic Trade Review* 1 (1): 18–25.
Cohen, Avner. 1998. *Israel and the Bomb*. New York, NY: Columbia University Press.
———. 2010. *Worst-Kept Secret: Israel’s Bargain with the Bomb*. New York: Columbia University Press.
Colby, Elbridge A., and Michael S. Gerson, eds. 2013. *Strategic Stability: Contending Interpretations*. Fort Belvoir, VA: Defense Technical Information Center. doi:10.21236/ADA572928.
Danzig, Richard. 2018. “Technology Roulette: Managing Loss of Control as Many Militaries Pursue Technological Superiority.” *Technology and National Security*, June.
de Villiers, J. W., Roger Jardine, and Mitchell Reiss. 1993. “Why South Africa Gave Up the Bomb.” *Foreign Affairs* 72 (5): 98–109.
Defense Innovation Unit. 2018. “Defense Innovation Unit (DIU) Annual Report.”
Demchak, Chris C. 1996. “Tailored Precision Armies in Fully Networked Battlespace: High Reliability Organizational Dilemmas in the `Information Age’.” *Journal of Contingencies and Crisis Management* 4 (2): 93–103. doi:10.1111/j.1468-5973.1996.tb00081.x.
———. 2003. “Creating the Enemy: Global Diffusion of the Information Technology-Based Military Model.” In *The Diffusion of Military Technology and Ideas*, edited by Emily O. Goldman and Leslie C. Eliason, 307–47. Stanford University Press.
———. 2018. “Four Horsemen of AI Conflict: Scale, Speed, Foreknowledge, and Strategic Coherence.” In *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives*, edited by Nicholas D Wright, 100–106. Strategic Multilayer Assessment Periodic Publication. https://nsiteam.com/social/wp-content/uploads/2019/01/AI-China-Russia-Global-WP_FINAL_forcopying_Edited-EDITED.pdf.
Dennis, Michael Aaron. 2013. “The Less Apparent Component—Tacit Knowledge as a Factor in the Proliferation of WMD: The Example of Nuclear Weapons.” *Studies in Intelligence* 57 (3). https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-57-no-3/the-less-apparent-component2014tacit-knowledge-as-a-factor-in-the-proliferation-of-wmd-the-example-of-nuclear-weapons.html.
D’Este, Carlo. 1983. *Decision in Normandy*. 1st ed. New York, NY: Dutton.
Etzkowitz, Henry, and Loet Leydesdorff. 2000. “The Dynamics of Innovation: From National Systems and ‘Mode 2’ to a Triple Helix of University–Industry–Government Relations.” *Research Policy* 29 (2): 109–23. doi:10.1016/S0048-7333(99)00055-4.
Flank, Steven. 1993. “Exploding the Black Box: The Historical Sociology of Nuclear Proliferation.” *Security Studies* 3 (2): 259–94. doi:10.1080/09636419309347549.
Forge, John. 2010. “A Note on the Definition of ‘Dual Use.’” *Science and Engineering Ethics* 16 (1): 111–18. doi:10.1007/s11948-009-9159-9.
Fuhrmann, Matthew. 2009. “Taking a Walk on the Supply Side: The Determinants of Civilian Nuclear Cooperation.” *Journal of Conflict Resolution* 53 (2): 181–208. doi:10.1177/0022002708330288.
Gady, Franz-Stefan. 2015. “New Snowden Documents Reveal Chinese Behind F-35 Hack.” *The Diplomat*. January 27. https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/.

Garfinkel, Ben, and Allan Dafoe. 2019. "How Does the Offense-Defense Balance Scale?" *Journal of Strategic Studies* 42 (6): 736–63. doi:10.1080/01402390.2019.1631810.
Gilli, Andrea, and Mauro Gilli. 2019. "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage." *International Security* 43 (3): 141–89. doi:10.1162/isec_a_00337.
Gordin, Michael D. 2009. *Red Cloud at Dawn: Truman, Stalin, and the End of the Atomic Monopoly*. New York: Farrar, Straus and Giroux.
Gowing, Margaret. 1964. *Britain and Atomic Energy, 1939-1945*. London, UK: Macmillan.
———. 1974a. *Independence and Deterrence: Britain and Atomic Energy, 1945-1952*. Vol. 2: Policy Execution. New York: St. Martin's Press. http://www.worldcat.org/oclc/1256196.
———. 1974b. *Independence and Deterrence: Britain and Atomic Energy, 1945-1952*. Vol. 1: Policy Making. New York: St. Martin's Press. http://www.worldcat.org/oclc/1256196.
Grissom, Adam. 2006. "The Future of Military Innovation Studies." *Journal of Strategic Studies* 29 (5): 905–34. doi:10.1080/01402390600901067.
Gusterson, Hugh. 2011. "The Assault on Los Alamos National Laboratory: A Drama in Three Acts." *Bulletin of the Atomic Scientists* 67 (6): 9–18. doi:10.1177/0096340211426631.
Hanham, Melissa, Catherine Dill, Jeffrey Lewis, Bo Kim, Dave Schmerler, and Joseph Rodgers. 2017. "Geo4nonpro.Org: A Geospatial Crowd-Sourcing Platform for WMD Verification." CNS Occasional Paper 28. Middlebury Institute of International Studies at Monterey.
Hecker, Siegfried S. 2008. "Denuclearizing North Korea." *Bulletin of the Atomic Scientists* 64 (2): 44–62. doi:10.1080/00963402.2008.11461145.
Holloway, David. 1996. *Stalin and the Bomb*. Yale University Press.
Horowitz, Michael C. 2010. *The Diffusion of Military Power: Causes and Consequences for International Politics*. Princeton, N.J: Princeton University Press. http://www.worldcat.org/oclc/761337088.
———. 2019. "When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence and Stability." *Journal of Strategic Studies* 42 (6): 764–88. doi:10.1080/01402390.2019.1621174.
Hymans, Jacques E. C. 2012. *Achieving Nuclear Ambitions: Scientists, Politicians and Proliferation*. Cambridge University Press.
Insinna, Valerie. 2019. "Inside America's Dysfunctional Trillion-Dollar Fighter-Jet Program." *The New York Times*, August 21, sec. Magazine. https://www.nytimes.com/2019/08/21/magazine/f35-joint-strike-fighter-program.html.
Jamrisko, Michelle, Lee J Miller, and Wei Lu. 2019. "These Are the World's Most Innovative Countries," January, 6.
Jervis, Robert. 1978. "Cooperation under the Security Dilemma." *World Politics* 30 (2): 167–214. doi:10.2307/2009958.
Joerges, Bernward. 1988. "Large Technical Systems: Concepts and Issues." In *The Development of Large Technical Systems*, edited by Renate Mayntz and Thomas P. Hughes, 9–36. Boulder, CO: Westview Press.
Johnston, Trevor, Troy Smith, and J. Irwin. 2018. *Additive Manufacturing in 2040: Powerful Enabler, Disruptive Threat*. RAND Corporation. doi:10.7249/PE283.
Jones, Brian. 2013. "The NSA Could Have Stopped Snowden If It Had More Bandwidth." *Business Insider*. October 18. https://www.businessinsider.com/the-nsa-could-have-stopped-snowden-if-it-had-more-bandwidth-2013-10.

Karpathy, Andrei. 2012. “The State of Computer Vision and AI: We Are Really, Really Far Away.” October 22. http://karpathy.github.io/2012/10/22/state-of-computer-vision/.
Kemp, R. Scott. 2014. “The Nonproliferation Emperor Has No Clothes.” *International Security* 38 (4): 39–78.
Kerr, Paul K., Steven A. Hildreth, and Mary Beth D. Nikitin. 2016. “Iran-North Korea-Syria Ballistic Missile and Nuclear Cooperation.” Report R43480. Congressional Research Service. http://digital.library.unt.edu/ark:/67531/metadc824727/?q=R43480.
Khan, Feroz Hassan. 2012. *Eating Grass: The Making of the Pakistani Bomb*. Stanford, California: Stanford University Press. http://www.worldcat.org/oclc/788269842.
Kiesler, Markey Hedy, and Antheil George. 1942. Secret communication system. United States US2292387A, filed June 10, 1941, and issued August 11, 1942. https://patents.google.com/patent/US2292387/en.
Korzekwa, Deniece. 2012. “Direct Casting Is the Future of Manufacturing Uranium Components.” *Actinide Research Quarterly*, no. 1 (October): 19–22.
Krepinevich, Andrew F. 1994. “Cavalry to Computer; the Pattern of Military Revolutions.” *National Interest*, no. 37 (Fall): 30–42.
———. 2002. *The Military-Technical Revolution: A Preliminary Assessment*. Center for Strategic and Budgetary Assessments. http://www.csbaonline.org/4Publications/Archive/R.20021002.MTR/R.20021002.MTR.pdf.
Kroenig, Matthew. 2010. *Exporting the Bomb: Technology Transfer and the Spread of Nuclear Weapons*. Ithaca: Cornell University Press.
Kroenig, Matthew, and Tristan Volpe. 2015. “3-D Printing the Bomb? The Nuclear Nonproliferation Challenge.” *The Washington Quarterly* 38 (3): 7–19. doi:10.1080/0163660X.2015.1099022.
Lewis, John Wilson, and Litai Xue. 1988. *China Builds the Bomb*. Stanford, CA: Stanford University Press.
Liberman, Peter. 2004. “Israel and the South African Bomb.” *The Nonproliferation Review* 11 (2): 46–80. doi:10.1080/10736700408436966.
Long, Janice R. 2015. “Chinese Cyber Espionage: A Complementary Method to Aid PLA Modernization.” Monterey, CA: Naval Postgraduate School.
Lucibella, Michael. 2015. “Manufacturing Revolution May Mean Trouble for National Security.” *American Physical Society*. April. https://www.aps.org/publications/apsnews/201504/revolution.cfm.
MacKenzie, Donald, and Graham Spinardi. 1995. “Tacit Knowledge, Weapons Design, and the Uninvention of Nuclear Weapons.” *American Journal of Sociology* 101 (1): 44–99. doi:10.1086/230699.
Marggraff, Melissa. 2015. “Next-Generation Manufacturing for the Stockpile.” *Science and Technology Review*, January, 4–11.
Mayntz, Renate, and Thomas Parke Hughes, eds. 1988. *The Development of Large Technical Systems*. Publications of the Max-Planck-Institut Für Gesellschaftsforschung, Köln. Frankfurt am Main : Boulder, Colo: Campus Verlag ; Westview Press.
McCarthy, John. 1990. “In Memoriam-Arthur Samuel: Pioneer in Machine Learning.” *AI Magazine* 11 (3): 10–11.
Meshkati, Najmedin. 1989. “Technology Transfer to Developing Countries: A Tripartite Micro- and Macroergonomic Analysis of Human-Organization-Technology Interfaces.”

International Journal of Industrial Ergonomics 4 (2): 101–15. doi:10.1016/0169-8141(89)90038-3.

Montgomery, Alexander H. 2005. "Ringing in Proliferation: How to Dismantle an Atomic Bomb Network." *International Security* 30 (2): 153–187.

———. 2013. "Stop Helping Me: When Nuclear Assistance Impedes Nuclear Programs." In *The Nuclear Renaissance and International Security*, edited by Adam N. Stulberg and Matthew Fuhrmann, 177–202. Stanford, CA: Stanford University Press.

Montgomery, Alexander H., and Tristan Volpe. 2017. "Hiding in Plain Sight? The Effect of Nuclear-Enabling Technologies on Strategic Surprise." Presented at the 58th Annual Convention of the International Studies Association. Baltimore, MD.

National Research Council. 2004. *Biotechnology Research in an Age of Terrorism*. National Academies Press.

Nelson, Amy J. 2015. "The Truth About 3-D Printing and Nuclear Proliferation." *War on the Rocks*. December 14. https://warontherocks.com/2015/12/the-truth-about-3-d-printing-and-nuclear-proliferation/.

———. 2019. "Innovation Acceleration, Digitization, and the Arms Control Imperative." SSRN Scholarly Paper ID 3382956. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3382956.

Office of Technology Assessment at the German Bundestag. 2017. "Additive Manufacturing (3D Printing)." TAB Policy brief 15. https://www.tab-beim-bundestag.de/en/news/20170918.html.

Ouagrham-Gormley, Sonia Ben. 2014. *Barriers to Bioweapons: The Challenges of Expertise and Organization for Weapons Development*. 1st ed. Cornell University Press. http://www.jstor.org/stable/10.7591/j.ctt1287dk2.

Padgett, John F. 2016. "The Emergence of Organizations and States," August. doi:10.1093/oxfordhb/9780190228217.013.2.

Panda, Ankit. 2018. "Exclusive: Revealing Kangson, North Korea's First Covert Uranium Enrichment Site." *The Diplomat*. July 13. https://thediplomat.com/2018/07/exclusive-revealing-kangson-north-koreas-first-covert-uranium-enrichment-site/.

Parayil, Govindan. 1991. "Schumpeter on Invention, Innovation and Technological Change." *Journal of the History of Economic Thought* 13 (1): 78–89. doi:10.1017/S1053837200003412.

Pietrucha, Mike. 2016. "The U.S. Air Force and Stealth: Stuck on Denial Part I," March, 8.

Pollack, Joshua. 2017. "Science, Advanced Industrial Technology, and Strategic Weapons Programs in North Korea." In *Evaluating WMD Proliferation Risks at the Nexus of 3D Printing and Do-It-Yourself (DIY) Communities*, edited by Robert Shaw, Ferenc Dalnoki-Veress, Shea Cotton, Joshua Pollack, Masako Toki, Ruby Russell, Olivia Vassalotti, and Syed Gohar Altaf, A95–106. James Martin Center for Nonproliferation Studies (CNS). https://www.jstor.org/stable/resrep17539.

Posen, Barry R. 1984. *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars*. Cornell Studies in Security Affairs. Ithaca, NY: Cornell University Press.

Purcell, Edward M., Carol G. Montgomery, and Dorothy Durfee Montgomery. 1952. Control of polarization in wave guides and wave guide systems. United States US2607849A, filed October 2, 1943, and issued August 19, 1952. https://patents.google.com/patent/US2607849A/en.

Putnam, Robert L. 2012. “A Look Back at the W88 Days.” *Actinide Research Quarterly*, no. 1 (October): 23–28.
Reed, Thomas C., and Danny B. Stillman. 2009. *The Nuclear Express: A Political History of the Bomb and Its Proliferation*. Minneapolis: Zenith Press. http://www.worldcat.org/oclc/209632366.
Reuters News. 2016. “China’s Midea Receives U.S. Green Light for Kuka Takeover,” December, 2.
Robbins, Martin. 2016. “Has a Rampaging AI Algorithm Really Killed Thousands in Pakistan?” *The Guardian*, February, 5.
Rochlin, Gene I. 1991. “Iran Air Flight 655: Complex, Large-Scale Military Systems and the Failure of Control.” In *Social Responses to Large Technical Systems : Control or Adaptation*, edited by Todd R. La Porte, 95–121. Dordrecht: Kluwer Academic Publishers.
———. 1998. “Trapped in the Net.” In *Trapped in the Net*, 218. Princeton, NJ: Princeton University Press.
Roff, Heather M. 2015. “Autonomous or `Semi’ Autonomous Weapons? A Distinction Without Difference.” January 16. http://www.huffingtonpost.com/heather-roff/autonomous-or-semi-autono_b_6487268.html.
Rublee, Maria Rost. 2009. *Nonproliferation Norms: Why States Choose Nuclear Restraint*. Athens: Univ. of Georgia Press. http://www.worldcat.org/oclc/300106928.
Ruttan, Vernon W. 1959. “Usher and Schumpeter on Invention, Innovation, and Technological Change.” *The Quarterly Journal of Economics* 73 (4): 596–606. doi:10.2307/1884305.
———. 2006. *Is War Necessary for Economic Growth?: Military Procurement and Technology Development*. Oxford University Press.
Santa Fe Institute Events. 2016. “SFI Innovation Short Course 2016 - A Theory of Invention and Innovation.” https://wiki.santafe.edu/index.php/SFI_Innovation_Short_Course_2016_-_A_theory_of_invention_and_innovation.
Scheinman, Lawrence. 1965. *Atomic Energy Policy in France under the Fourth Republic*. Princeton, NJ: Princeton University Press. http://www.worldcat.org/oclc/237022.
Schelling, Thomas C. 1960. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press.
Schneider, Jacquelyn. 2019. “The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War.” *Journal of Strategic Studies* 42 (6): 841–63. doi:10.1080/01402390.2019.1627209.
Sechser, Todd S., Neil Narang, and Caitlin Talmadge. 2019. “Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War.” *Journal of Strategic Studies* 42 (6): 727–35. doi:10.1080/01402390.2019.1626725.
Slayton, Rebecca. 2017. “What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment.” *International Security*, February. doi:10.1162/ISEC_a_00267.
Talmadge, Caitlin. 2019. “Emerging Technology and Intra-War Escalation Risks: Evidence from the Cold War, Implications for Today.” *Journal of Strategic Studies* 42 (6): 864–87. doi:10.1080/01402390.2019.1631811.
Tirone, Daniel C., and James Gilley. 2015. “You Can Print Your Own Guns at Home. Next It Will Be Nuclear Weapons. Really.” *Washington Post*, September. http://www.washingtonpost.com/blogs/monkey-cage/wp/2015/09/07/you-can-print-your-own-guns-at-home-next-it-will-be-nuclear-weapons-really/.

Trucano, Michael, and Gavin Dykes. 2017. "Building and Sustaining National Educational Agencies: Lessons, Models and Case Studies from around the World." World Bank. saber.worldbank.org.
UNIDIR. 2014. "Framing Discussions on the Weaponization of Increasingly Autonomous Technologies."
U.S. Department of Defense. 2014. "Department of Defense Strategy for Countering Weapons of Mass Destruction." Office of the Deputy Assistant Secretary of Defense for Countering Weapons of Mass Destruction. http://archive.defense.gov/pubs/DoD_Strategy_for_Countering_Weapons_of_Mass_Destruction_dated_June_2014.pdf.
Volpe, Tristan A. 2019. "Dual-Use Distinguishability: How 3D-Printing Shapes the Security Dilemma for Nuclear Programs." *Journal of Strategic Studies* 42 (6): 814–40. doi:10.1080/01402390.2019.1627210.
Way, Christopher, and Jessica Weeks. 2014. "Making It Personal: Regime Type and Nuclear Proliferation." *American Journal of Political Science* 58 (3): 705–19. doi:10.1111/ajps.12080.
Williams, Heather. 2019. "Asymmetric Arms Control and Strategic Stability: Scenarios for Limiting Hypersonic Glide Vehicles." *Journal of Strategic Studies* 42 (6): 789–813. doi:10.1080/01402390.2019.1627521.
Wise, David. 2011. "China's Spies Are Catching Up." *The New York Times*, December 10, sec. Opinion. https://www.nytimes.com/2011/12/11/opinion/sunday/chinas-spies-are-catching-up.html.
Work, Robert. 2015. "The Third U.S. Offset Strategy and Its Implications for Partners and Allies." Deputy Secretary of Defense Speech, Willard Hotel, Washington DC, January 28. https://www.defense.gov/Newsroom/Speeches/Speech/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies/.
Xinhua. 2019. "China Bucks Global Trend with Record FDI Inflows in 2018: UN Report." June 13. http://www.xinhuanet.com/english/2019-06/13/c_138138291.htm.
Yanqiong, Liu, and Liu Jifeng. 2009. "Analysis of Soviet Technology Transfer in the Development of China's Nuclear Weapons." *Comparative Technology Transfer and Society* 7 (1): 66–110. doi:10.1353/ctt.0.0023.