Deloitte.
Insights

A report from the
Deloitte Center for Government Insights

National security and technology regulation

Government regulations for emerging technology

About the authors

Henry Ennis | hennis@deloitte.com

Henry Ennis is a senior manager in Deloitte Consulting LLP's Government and Public Services Strategy and Analytics practice. Ennis brings over a decade of experience framing issues and defining and implementing enterprise strategies to address nascent and evolving national security matters. He has worked at the intersection of international finance, public policy, and national security since 2011, including defining and executing programs to comply with national security agreements between government and industry, and identifying opportunities to optimize CFIUS-related operations for the federal government. He has also worked extensively with government, industry, and NGOs in the Americas, Middle East, Africa, and South Asia in the area of investment facilitation.

Alan Estevez | alanestevez@deloitte.com

Alan Estevez is a specialist executive with Deloitte Consulting LLP. He had a 36-year career with the Department of Defense (DoD) that culminated in two senate-confirmed positions serving the president of the United States under four secretaries of defense. He's reliably solved vast problems with novel methods, earning multiple DoD Distinguished Public Service Medals, two Presidential Rank Awards, and the Service to America medal. As principal deputy undersecretary of defense for acquisition, technology, and logistics, Estevez oversaw more than 40,000 people, a US$20 billion budget, and an annual contract spend of US$300 billion. He led support to operations in Iraq and Afghanistan, piloted contingency and humanitarian efforts including Hurricane Sandy relief and the West Africa Ebola mission, and represented the DoD on the Committee on Foreign Investment in the United States (CFIUS).

Joe Mariani | jmariani@deloitte.com

Joe Mariani is a research manager with Deloitte's Center for Government Insights. His research focuses on innovation and technology adoption for both commercial businesses and national security organizations. His previous experience includes work as a consultant to the defense and intelligence industries, high school science teacher, and Marine Corps intelligence officer.

Jessica Moran | jesmoran@deloitte.com

Jessica Moran is a senior consultant with Deloitte & Touche's Defense, Security & Justice practice. Her research interest focuses on enhancing legal and regulatory frameworks to support national security objectives. She holds a BA from the College of the Holy Cross, a JD from the College of William and Mary, and is pursuing an LLM in national security from Georgetown.

Joe Pauloski | jpauloski@deloitte.com

Joe Pauloski is a national security and defense professional within Deloitte Consulting LLP currently supporting the Committee on Foreign Investment in the United States at the Department of the Treasury. His analysis aids the review of foreign investment in critical technologies. Pauloski's previous experience includes conducting supply chain risk analysis for domestic and foreign clients and contracting at the Pentagon in a variety of roles in support of defense acquisition, technology, and logistics.

Contents

Introduction

A swarm of drones patrols the battlespace, guided by sensors originally developed for smart factories. An artificial intelligence algorithm developed for online gaming steers military commanders toward smarter, faster decision-making. Ubiquitous cameras and ample cloud storage bring facial recognition to every street corner, but they can be used for both assessing threats in airports as well as to identify intelligence operatives.

WHILE THESE SCENARIOS may sound like a trailer for this summer's futuristic blockbuster movie, emerging dual-use technologies are making such seemingly fantastical plots the reality of our world. The foundations for these technologies were developed for commercial uses and are readily available for consumers on the open market. However, the acceleration in innovation and technology, particularly in the commercial sector, creates challenges for those who need to regulate them.[1]

There are innumerable examples of how commercial-origin technology can have unintended national security consequences—and how our current regulatory regime has not yet adapted for this new reality in order to keep such capabilities out of the hands of hostile actors. A precursor to protecting critical technologies is identifying what technologies are, in fact, critical. This article starts to address this question by exploring ways in which regulators could better define and protect the critical while still enabling future innovation, growth, and development of technology. To do so, governments may need to ask new questions, form new partnerships, and adopt new processes to keep pace with emerging technologies.

The complications of emerging technology

SINCE THE 1950S, the United States has depended on its technological advantage as a key component of national security.[2] To retain that edge and support the industries that created it, the United States adopted rules to regulate national security technologies. In the past, such technologies were largely developed by a handful of well-known companies that formed the traditional military industrial base, making it easy to identify national security-relevant technologies.

Today, the rate of technological change means that such technologies are increasingly likely to come from companies with purely commercial intentions. For example, in 2016, commercial companies invested more than double federal R&D funding, a dramatic reversal from the 1960s when government funded more than 50 percent of all R&D.[3] The growth in purely-commercial technology can make it difficult to even identify which technology could have national security implications. It also means that technologies are evolving more quickly than the regulatory regimes put in place to control them. The result is that the battlefields of the future may be as dependent on commercial-origin technology as they are on bombs and bullets. This fact necessitates a fundamental change in how we approach the acquisition and regulation of technologies related to national security.

Today, the rate of technological change means that such technologies are increasingly likely to come from companies with purely commercial intentions.

The challenge for both the process and players

The current, well-established frameworks that control the flow of dual-use technologies coming out of government or aerospace and defense industry may be less effective at controlling technologies that emerge from areas less traditionally associated with national security. The United States, for example, has a robust, though bifurcated, regime for preventing the diffusion of traditional defense or dual-use technologies deemed critical to national security.

Exports of certain technologies are limited under the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). Under ITAR, the Department of State manages the export of dedicated military technologies with the United States Munitions List (USML), while additional regimes and international law frameworks support nonproliferation of nuclear, chemical, biological, and missile technologies.[4]

Similarly, the EAR regulates across the spectrum of dual-use technologies.[5] This complex regulatory regime also includes the review of foreign investment within the United States by the Committee on Foreign Investment in the United States (CFIUS),[6] the regulation of the federal supply chain,[7] and, if necessary, the authority to impose economic sanctions on foreign countries by the Department of the Treasury's Office of Foreign Assets Control.[8]

Together, these controls have effectively controlled the proliferation of nuclear, chemical, and other sensitive technologies around the globe. But with so many companies, government agencies, and nongovernmental organizations involved in the development, use, and control of new technologies, it can be difficult to navigate the differing postures on how regulation should be conducted and what a national security technology even is—let alone figure out who is relevant to what discussions on the regulation of said technology.

For example, the Department of Defense's (DOD's) focus is national security and protecting the war fighter. When translating this mission to national security technologies, the DOD will, naturally tend to lean toward greater controls over technology, which may harm national security. In contrast, part of the Department of the Treasury's mission is to promote the conditions that enable economic growth and stability, which may often correspond to a freer, less controlled flow of technology. While these objectives don't necessarily conflict, taken together, they make for a complex dynamic. Additionally, an agency's focus can also evolve: the US Trade Representative, traditionally a free market–focused entity, now cites national security concerns to support tariffs on steel and aluminum.[9]

Each of these different regulatory players bring different perspectives even on basic questions such as which technologies are relevant to national security. Some may define national security technologies as anything that grows the economy while others may take a narrower definition by restricting it only to technologies likely to be found on the battlefield. Traditionally, dual-use items are analyzed for export under the EAR based on three factors: end use, end user, and end location.[10] However, each of these three factors becomes harder to identify with commercial-origin technologies. When computer code is in the cloud, where is the location of the end user? What is the end use of gene therapy: providing life-saving treatment for a genetic disorder or delivering a life-threatening toxin? Regulatory tools built for explosives, jet fighters, and nuclear weapons may not be the best fit for the task. The result is that even the narrowest definition of national security technologies can force regulators to grapple with commercial-origin technologies.

New tech, old rules, new problems

SO WHAT ARE regulators to do? For a technologist, a drone is a brilliant business-to-consumer product that can enable advances in customer service. For a national security proponent, it is a highly accurate and autonomous targeting software that could enable a militarized unmanned aerial vehicle (UAV) to track an asset or scout a location. Regulators cannot simply ban the technology; the commercial benefit is too great. The technology could lead to a thriving global industry for increasingly specialized and capable UAVs, systematically adding value to industry in every sector. In fact, with commercial operators already approved to deliver packages in many countries, regulators may not even be able to control the flow of the technology. It is already out in the wild. However, regulators cannot simply remain passive, given the potential that some bad actors may use such technologies to develop military applications.

The current processes do not generally afford the flexibilities to optimally deal with these new technologies.

Governments rightly want to regulate the diffusion of these emerging technologies. Some technologies, however, are difficult to regulate while preserving the advancement of both economic growth and domestic military interests. Attempting to close the open exchange of ideas between industry, academics, and independent researchers could stifle innovation, hurting both US businesses *and* national security interests that may require these technologies in the future.

The current processes do not generally afford the flexibilities to optimally deal with these new technologies. That mismatch can create five challenges:

1. Evolving tech

Not only is the constant emergence of new technologies a challenge to regulation, but existing technologies are not standing still either. Even centuries-old technologies like the engine in your car have seen dramatic innovation in the last decade, resulting in double the fuel efficiency and half the carbon dioxide emissions seen in 1975.[11] This can become a significant issue when a shift in underlying technology changes how a system performs. Take quantum computing, for example. The same basic collection of logic gates used in traditional computing, when applied to quantum bits, can produce entirely new results. Where traditional computing bits are either 1 or 0, on or off, quantum bits can exist across a number of states, allowing quantum computers to work probabilistically and answer questions in a different manner than traditional computers. That subtle change in the underlying technology of how a computer works can allow quantum computers to break encryption algorithms in a few hours or days that would take traditional computers the lifetime of the universe to crack.[12] The consequences of even small evolutions in technology can have significant impacts on security.

THE WINDING ROAD OF SELF-DRIVING CARS

While we typically think of them as a Silicon Valley innovation, self-driving cars were actually fostered by the Defense Advanced Research Projects Agency (DARPA) research from the 1960s through to the Grand Challenges of the 2000s, which spurred teams of innovators to develop autonomous vehicles that could compete for prize money—and pride.[13] Further, many of the innovations that make self-driving cars possible, such as LiDAR sensors, were also developed with US government backing. While the growth of the self-driving car industry represents an enormous positive externality of the government efforts, the diffusion of the technologies involved may also present some risk. In the race for full autonomy, even fully commercial uses of the technology will have profound implications for future warfare just as the automobile replacing the horse had massive implications for military logistics.

2. New producers

The Defense Industrial Base has long encompassed both military and commercial technologies. For example, the same companies that produce fighter jets also make commercial airliners. What is different today is that now purely commercial companies with no interest in defense are finding themselves subject to national security regulations simply due to the unforeseen applications of their products. This can pose a challenge to regulators who both need to identify those technologies and work with companies that may have less vested interest in complying with national security regulations. Take graphene, the single-atom-thick layer of carbon, as one example. When it was discovered at the University of Manchester in 2004, graphene was nothing more than just a smudge on a piece of tape, certainly nothing to arouse the interest of national security regulators.[14] However, 15 years later, graphene is poised to revolutionize everything from aircraft wings to electronics, drug delivery to motor oil. Today, the potential of graphene to create 45 percent more efficient Li-ion batteries that charge in 12 minutes alone would be enough to warrant the attention of regulators.[15]

3. Unforeseen applications

Another challenge is how quickly the uses of technology can change. A technology that emerged to serve a purely commercial need, and therefore not in the purview of regulation, can quickly have unforeseen implications for defense or national security. Think of the short leap from 3D printing small curios to printing weapons and other dangerous items. In 2013, a student 3D printed a plastic gun that could fire live rounds and published the blueprints online. In 2016, the Transportation Security Administration (TSA) found a 3D printed revolver in carry-on luggage. Even nontraditional

HOW MOVIE-MAKING TECHNOLOGY BECAME A NATIONAL SECURITY CONCERN: THE STORY OF DEEPFAKES

Deepfakes are lifelike videos that use AI to study and then mimic human beings. They can be so convincing that many viewers would not be able to immediately discern that they are not watching a real human, but rather a hyper-accurate digital rendering. The potential to unleash this technology for the purpose of influence operations makes it of legitimate national security concern as shown when comedian and film director Jordan Peele created a fake video of President Obama.[16] They can be so convincing, in fact, that some leading researchers have changed their sharing practices and now limit what they publish publicly, which is not required by regulation.[17] A few years ago, this would have been taboo for many computer scientists who typically prize open source collaboration.

weapons can be printed—in 2015, a plasma railgun that could fire projectiles at a speed of 560 mph was made using a 3D printer.[18] Additive manufacturing is revolutionizing manufacturing in the commercial sector and is being increasingly seen as a solution to improve military readiness;[19] however, without regulation, it can lead to dangerous applications in the hands of bad actors.

4. Time lag

Perhaps the single greatest challenge to regulating commercial-origin technologies is simply the pace of technological advancement. Today, new technologies are emerging almost daily. The average life span of software is four to six years, with smaller apps lasting less than half of that.[23]

Regulation, on the other hand, operates on much longer time cycles. For example, the EAR and ITAR export regimes were largely established during the 1970s. But it wasn't until 2009 that serious reforms were undertaken.[24] Similarly, the rules on foreign investment in sensitive technologies set out in the Foreign Investment and National Security

INNOCENT INNOVATION OR MILITARY MENACE?

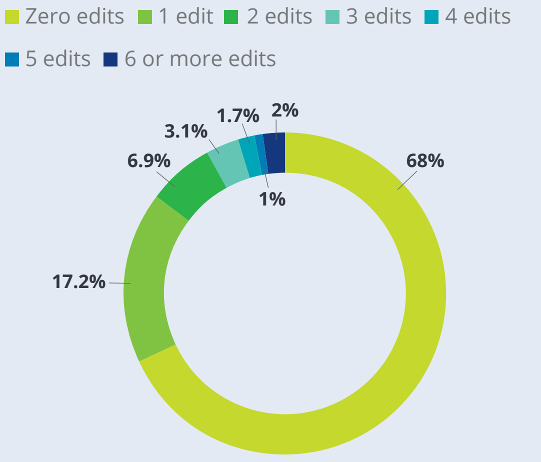
Some intelligent drone applications can drive real progress for industry. In agriculture, drones are increasingly able to assess soil quality and terrain, monitor crops for diseases, and assess microclimates within greenhouses.[20] In urban planning, construction, and heavy industry, drones can capture 2D imagery and generate 3D renderings and thermal images to drive safer, more accurate building plans.[21] In warehouse management, drones can scan inventory and at large sporting events, drones can track and evaluate individual players in real time.[22] The trouble is that every one of these novel uses for industry can also have unintended security consequences. Rather than the image processing being used for agricultural drones, it can be used to spot camouflaged facilities. Image tagging and 3D renderings can be invaluable tools for clandestine intelligence collection, while facial recognition in crowds can be a key surveillance tool to identify dissidents or spies.

THE LONELY LIFE OF A REGULATION

The challenge of making timely regulation is not just the time it takes to pass legislation or publish rules. But another factor likely exacerbating the problem is how rarely regulations are changed or updated once published (see figure 1). Our analysis of the 2017 US Code revealed that 68 percent of federal regulations were never updated once published.[25] While this may have worked in other eras, today the rapid pace of technological change seems to have shattered the assumption that regulations can remain unchanged for decades.

FIGURE 1

US regulations are rarely revised once published



Source: Deloitte Center for Government Insights analysis.

Act of 2007 were not meaningfully changed until the Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018. To put that in perspective, five entire generations of mobile software could have been introduced, used, and discarded for the next tool in that span. Clearly, regulators should consider new, faster methods if they are to keep pace with the technologies they wish to regulate.

5. Many regulators

As the number and diversity of technology creators increases, the uses to which those technologies can be put also proliferate. More creators, more industries, more uses, all mean that any given technology has the potential to touch many different regulators. Take flying cars, for example. These could need certification or oversight ranging from the Federal Aviation Administration (FAA) since they fly through congested airspace, the Department of Transportation since they drive on public roads, Department of Homeland Security or even Customs and Border Patrol if crossing borders, plus many others. The challenge is that all of these different regulators come with different perspectives and goals that drive how they approach the regulation of technology.

Organizing all of these different players by their role and general perspective can be helpful merely as a map of the space in which regulation of emerging technology exists. In terms of role, organizations can be either builders or regulators of technology. However, perhaps the largest expansion of this map comes from the perspective or focus of organizations. While the traditional defense industrial base certainly had both a security and market focus—making both fighter jets and commercial airliners, for example—today technologies with security implications are just as likely to arise from companies with no clear connection to or interest in security.[26] Take the weaponization of social media or unintended use of 3D printers to make weapons as examples. This not only introduces new builders to the national security technology landscape, but also the regulators who traditionally oversaw those technologies.

FIGURE 2

Many players are involved in regulating national security technologies

	Security focus	Market focus
Regulators	Departments of State, Homeland Security, Defense, and Justice	Departments of Commerce and Treasury, trade representatives, consumer and safety regulators, etc.
Builders	Traditional military industrial base	
	Government labs, federally funded R&D centers, etc.	Other industries, academia, and other technology producers

Source: Deloitte analysis.

MORE PLAYERS CALLS FOR WIDER ENGAGEMENT

With so many new players—both regulators and builders—touching national security technologies today, wider engagement is needed across all of those players to control the negative uses of such technologies. This trend is perhaps clearest in efforts to counter enemy disinformation. During the Cold War, the gold standard for countering disinformation and propaganda was the Active Measures Working Group (AMWG). The AMWG, formed in the 1980s, brought together subject matter experts from the State Department, the US Information Agency, the CIA, the FBI, and even congressional staffs. The group worked as an information broker across the federal government to identify, track, and develop strategies to successfully counter Soviet disinformation campaigns in the United States and abroad.[27]

The analog of Soviet propaganda today is coordinated, inauthentic behavior on social media platforms. By creating fake accounts or posting dubious claims, governments and groups can misuse commercial technology to try and influence large amounts of people very quickly. A recent NATO report on such activity shows that only two years ago, up to 70 percent of social media posts about NATO were bots or other inauthentic activity, demonstrating just how important this problem can be to military and defense matters.[28]

However, where the AMWG simply had to operate in a network of a handful of government agencies, today's regulators must operate across much wider networks that include the creators of the technology itself. For example, NATO would not make much progress on countering social media propaganda without the social media companies themselves. These companies are best positioned to understand how nefarious AI bots operate on their networks; to that end, Facebook removes 1 million fake accounts a day, while Twitter challenges 8.5–10 million accounts a week.[29]

The future of regulation is today

New regulatory rules could help to overcome these challenges and effectively control potential threats from new technologies without stifling innovation. Government should not only work within an integrated, informed network of regulators and tech producers, but also consider finding new ways to simultaneously build and regulate technology. Those new tools and new ways of regulating can be summarized as *The future of regulation*.

This new approach seeks to guide the development of technologies in the right direction with adaptive approaches to regulation. Technologies are advancing rapidly in ways we can't always predict and, if adopted, the future of regulation offers new tools and approaches that can help address each of the challenges posed by new, commercial-origin technologies (see figure 3).

1. Managing evolving technology with outcomes, not rules

The challenge with evolving technology is that it constantly changes the mechanism of a problem. To counter this, regulators should focus on the outcomes they hope to achieve rather than the technology responsible for it. So today, the speed limit regulates the outcome of how a car is driven—not the top speed capability or horsepower of the technology. The same approach can be useful with new technologies as well.

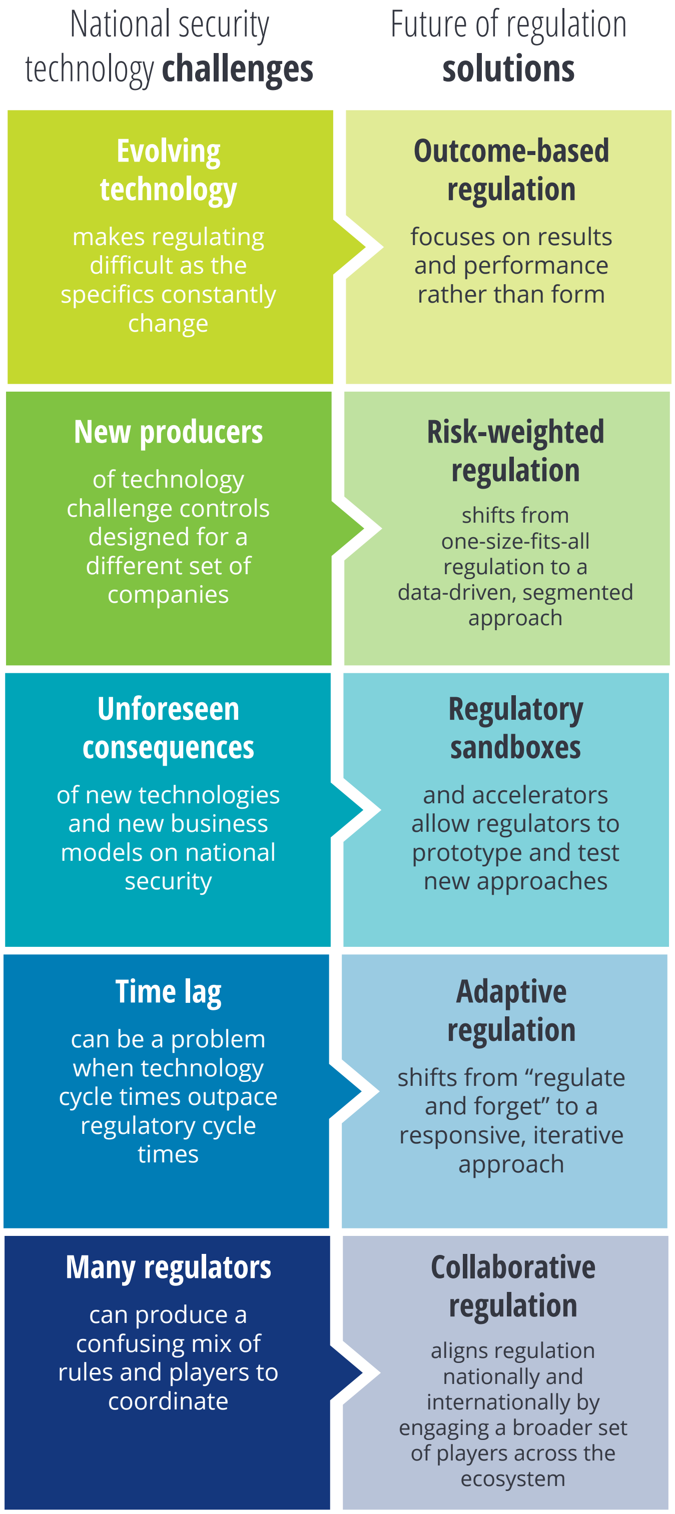
Take the shift from model aircraft to drones. While both are small, unmanned aircraft controlled remotely from the ground, the low cost and high performance of commercial drones have made them explode in popularity compared to the much smaller model aircraft community. The different rules concerning model aircraft and drones often lead to confusion about what was required of operators of each. But with Section 349 of the 2018 FAA Reauthorization, rules now focus on desired outcomes of safe operation such as not flying over crowds or beyond a pilot's capability to control the drone and not on the specific technology being flown.[30]

2. Assessing technologies with risk-based regulation

The increase in the variety of players involved in developing and regulating national security technologies can bring with it a variety of different, competing priorities as well. A risk-based approach to regulation can help to balance those competing priorities. Such a system could include a risk-based approach where rules and restrictions are based on a custom assessment of whether the risk posed by a company or technology exceeds certain thresholds. This is the approach taken by the final version of FIRRMA.[31] While regulators previously evaluated which countries may have posed significant threats to technology, the new rules allow for a risk-based approach to individual investors or companies.[32] This approach can help regulators focus efforts on areas of concern as they sift through thousands of undeclared, yet critical transactions. Plus, aside from allowing regulators to be more efficient with limited resources, this approach can also minimize unnecessary barriers to funding for young companies, encouraging the development of new technology.

FIGURE 3

The future of regulation offers new tools and approaches that can help address the challenges posed by new commercial technologies



National security technology **challenges**	Future of regulation **solutions**
Evolving technology makes regulating difficult as the specifics constantly change	**Outcome-based regulation** focuses on results and performance rather than form
New producers of technology challenge controls designed for a different set of companies	**Risk-weighted regulation** shifts from one-size-fits-all regulation to a data-driven, segmented approach
Unforeseen consequences of new technologies and new business models on national security	**Regulatory sandboxes** and accelerators allow regulators to prototype and test new approaches
Time lag can be a problem when technology cycle times outpace regulatory cycle times	**Adaptive regulation** shifts from “regulate and forget” to a responsive, iterative approach
Many regulators can produce a confusing mix of rules and players to coordinate	**Collaborative regulation** aligns regulation nationally and internationally by engaging a broader set of players across the ecosystem

Source: Deloitte Center for Government Insights analysis.

3. Mitigating unforeseen circumstances by building sandboxes

As new technologies spread, they can uncover unexpected uses. Often these can be positive, such as the discovery that wallpaper cleaning paste was a fun toy for children, leading to Play-Doh.[33] Other times the new uses can lead to negative consequences that need to be controlled, such as disinformation on social media or bomb-carrying hobby drones. But how can regulators possibly know ahead of time what these unforeseen uses may be? One answer is to put those technologies to actual use in safe environments, or "sandboxes," to find out.

A sandbox can sound like an unfamiliar, high-tech term, but it is actually a concept the national security community has long experience with. For example, in 2016 the Marine Corps designated its first experimental unit, an infantry battalion that would remain a part of the operating force but would be tasked with testing new technology and concepts during its exercises and deployments.[34] This allowed the Marine Corps to test technologies and iron out any issues away from combat before scaling them to the entire force. The experimental unit was key to the fielding of new mini-quadcopters and new organizational structure for the infantry squad. In fact, it has proved so successful that the program is continuing with experimental units in other fields such as logistics.[35]

4. Combatting time lag with adaptive regulation

With the cycle time for commercial technology ever decreasing, the current regulatory framework is perhaps better suited to the 67-year-old B-52 than the commercial-origin technology that will become increasingly relevant in the battlefields of the future. To keep up with the pace of technological change requires regulations that can adapt and adjust with the technology.

One successful example of adaptive regulation is the National Institute of Standards and Technology's (NIST's) Cybersecurity Framework (CSF). Based on an executive order to reduce cyber risk to our critical infrastructure, NIST engaged with industry to identify standards, guidelines, and best practices before issuing CSF version 1.0 in 2014.[36] But it did not stop at the publication of the first set of standards, NIST continually engages with the public through workshops, requests for comment, and other means to understand how technology and threats are changing. The result is that they can update standards to provide continually evolving, accurate guidance even as technology changes.[37]

5. Achieving interoperability through collaborative regulation

Many regulators, many technology producers in many industries can lead to a tangled web of rules that can be difficult to navigate in the best of times. One solution is collaborative regulation where regulators in different areas work together to create a consistent set of rules across industries, technologies, and even international borders.

One example of such collaborative regulation is the recent announcement of the Trusted Capital Marketplace, which is a public-private partnership designed to link private sources of capital with innovative startups in need of funding.[38] CFIUS and other national security controls seek to prevent foreign investment in critical technologies, but this approach may also have the unintended consequence of starving nascent technologies of needed capital. The new marketplace creates an online space where small- and medium-sized companies that may otherwise have gone out of business or had to seek foreign investment can find trusted sources of capital. By collaborating with tech producers, investors, and other stakeholders, this approach can harmonize the goals of both protecting and supporting new technologies.

How to get started today to address tomorrow's threats

SUPPORTING THE DEVELOPMENT of national security technologies and keeping those technologies from adversaries is a key factor in any nation's comparative advantage. More than any particular enforcement strategy or rule, striking the right balance between those twin goals requires a deep understanding of how technology may be used today, and evolve tomorrow. This is only possible when the multiplex of regulators collaborates as one, and with technology producers, they must regulate.

Government agencies and technology producers have more in common than it may seem. Government wants to prevent the exploitation of national security technologies while technology producers don't want their technologies misused. Similarly, technology producers primarily want to bring their new technologies to the world, and government too recognizes the importance of continued technological development. The principle for regulation of national security technologies builds on this common ground to create an adaptive, collaborative approach to protecting security and encouraging technology at the same time.

But such collaborative regulation is only possible when different regulators and technology producers trust each other. When teams share trust, then they can recognize their shared purpose. This mentality can lead to increased efficiency and interoperability toward a common goal. This cultural shift is similar to that which occurred within the intelligence community following 9/11. In the wake of the 9/11 Commission report, Congress established a number of cross-cutting organizations, common training requirements, and other reforms across a variety of agencies and programs.[39] The results were impressive, with the former Director of National Intelligence observing that, "we now collaborate on intelligence collection and analysis in ways that were unheard of 10 years ago."[40] Therefore, the first step toward more collaborative regulation of national security technologies is to establish communities of trust across different regulators and technology producers, both domestic and international. As trust and interoperability grow, opportunities for further integration—the use of shared data, for example—can become natural progressions.

Establishing trust can seem like a difficult first step, but the stakes have never been higher. New commercial-origin technologies may become so pervasive that they could have the potential to undermine the very core of democracy in a way explosives or chemical weapons never could. How the United States approaches its regulation of these powerful technologies today will have lasting impacts on our future security and on the world.

Endnotes

1. We will use the term "commercial-origin" or "dual-use" technologies throughout this article to refer to the class of technologies that emerged from industry to solve purely commercial problems but ended up having unintended security uses or implications. This is as opposed to other dual-use technologies that emerged from government but ended up having commercial applications, such as nuclear technology.
2. Katie Lange, "3rd Offset Strategy 101: What it is, what the tech focuses are," *Chips*, March 30, 2016.
3. Ana Maria Santacreu and Heting Zhu "R&D: Business spending up, government spending flat," Federal Reserve Bank of St. Louis, May 14, 2018.
4. Arms Export Control Act, as amended, 22 U.S.C. § 2778. International Traffic in Arms Regulation, 22 CFR §§120–130.
5. Export Administration Act of 1979, as amended, and replaced by the Export Controls Act of 2018, Pub. L. No. 115–232 (2018).
6. US Department of the Treasury, "The Committee on Foreign Investment in the United States (CFIUS)," accessed June 18, 2019.
7. Congress.gov, "John S. McCain National Defense Authorization Act for Fiscal Year 2019," accessed June 18, 2019.
8. See US Department of the Treasury, "Financial sanctions," accessed June 18, 2019.
9. Associated Press, "The latest: Tariff agreement hailed by business groups," May 18, 2019.
10. Bureau of Industry and Security, "Export Administration Regulations," accessed June 18, 2019.
11. US Environmental Protection Agency, "The 2018 EPA automotive trends report," March 2019.
12. Edward Gerjuoy, "Shor's factoring algorithm and modern cryptography: An illustration of the capabilities inherent in quantum computers," *American Journal of Physics* 73, no. 6 (2005): DOI: https://doi.org/10.1119/1.1891170.
13. Alex Davies, "Inside the races that jump-started the self-driving car," *Wired*, November 10, 2017.
14. Steve Connor, "The graphene story: How Andrei Geim and Kostya Novoselov hit on a scientific breakthrough that changed the world…by playing with sticky tape," *Independent*, March 18, 2013.
15. GSMA, "Global mobile radar," September 2018.
16. James Vincent, "Watch Jordan Peele use AI to make Barack Obama deliver a PSA about fake news," Verge, April 17, 2018.
17. CNN, "When seeing is no longer believing," accessed May 23, 2019.
18. John Hornick, "How criminals are using 3D printing," PoliceOne, September 13, 2017.
19. Dustin Q. Diaz, "MAKE Lab opens bringing new AM opportunities to NSWC Carderock Division," Naval Sea Systems Command, April 5, 2016; Matt Gonzales, "3D-printed impeller enhances readiness of Corps' main battle tank," Defense Logistics Agency, April 4, 2019.
20. Joe Mariani and Junko Kaji, "From dirt to data: The second green revolution and the Internet of Things," *Deloitte Review* 18, January 25, 2016.
21. David Schatsky and John Ream, *Drones mean business: Advanced software applications are driving commercial drone adoption*, Deloitte Insights, December 5, 2016.

22. Deloitte, “Drones: High-profile and niche,” accessed June 18, 2019.

23. MitoSystems, “Software evolution,” accessed April 23, 2019.

24. Export.gov, “About Export Control Reform (ECR),” accessed June 18, 2019.

25. William Eggers, Mike Turley, and Pankaj Kishnani, *The future of regulation: Principles for regulating emerging technology*, Deloitte Insights, June 19, 2018.

26. In 2018, agencies of the US government were awarded less than 4,000 patents, which is less than half of the top commercial patent awardees.

27. Fletcher Schoen and Christopher J. Lamb, “Deception, disinformation, and strategic communications,” Institute for National Strategic Studies, Strategic Perspectives 11, 2012.

28. For current statistics, see NATO Strategic Communications Center of Excellence, “Robotrolling,” 2019. For historical numbers, see Smarter Every Day, “Who is manipulating Twitter?,” YouTube, April 8, 2019.

29. For Facebook, see Queenie Wong, “Facebook’s AI helping block or remove 1 million accounts a day,” CBS News, April 8, 2019. For Twitter, see Yoel Roth and Del Harvey, “How Twitter is fighting spam and malicious automation,” Twitter Blog, June 26, 2018.

30. Federal Aviation Administration, “FAA highlights changes for recreational drones,” May 16, 2019.

31. Jeff Farrah, “Foreign Investment Bill and its impact on the VC and startup ecosystem,” NVCA blog, July 25, 2018.

32. Lathan & Watkins LLP, “Overview of the CFIUS process,” accessed June 18, 2019.

33. Tim Walsh, *Timeless Toys: Classic Toys and the Playmakers Who Created Them* (Kansas City: Andrews McMeel Publishing, 2005).

34. Hope Hodge Seck, “Marines designate infantry battalion as new experimental unit,” Military.com, accessed June 18, 2019.

35. Hope Hodge Seck, “The Marine Corps just announced its next experimental unit,” Task & Purpose, January 4, 2018.

36. National Institute of Standards and Technology, “Cybersecurity framework,” accessed June 18, 2019.

37. National Institute of Standards and Technology, “Evolution of the framework,” accessed June 18, 2019.

38. Scott Maucione, “DoD to help trusted companies and investors meet to build industrial base,” Federal News Network, May 10, 2019.

39. National Commission on Terrorist Attacks, “The 9/11 Commission report,” accessed June 18, 2019.

40. Office of the Director of National Intelligence, “DNI Clapper OP-ED in the Wall Street Journal: How 9/11 transformed the intelligence community,” press release, September 7, 2011.

Acknowledgments

The authors would like to thank **Isaac Jenkins** for his invaluable contributions to this effort.

About the Deloitte Center for Government Insights

The Deloitte Center for Government Insights shares inspiring stories of government innovation, looking at what's behind the adoption of new technologies and management practices. We produce cutting-edge research that guides public officials without burying them in jargon and minutiae, crystalizing essential insights in an easy-to-absorb format. Through research, forums, and immersive workshops, our goal is to provide public officials, policy professionals, and members of the media with fresh insights that advance an understanding of what is possible in government transformation.

Deloitte offers national security consulting and advisory services to clients across the Department of Homeland Security, the Department of Justice, and the intelligence community. From cyber and logistics to data visualization and mission analytics, personnel, and finance, we bring insights from our client experience and research to drive bold and lasting results in the national security and intelligence sector. People, ideas, technology, and outcomes—all designed for impact. Read more about our national security services on Deloitte.com.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Practice leadership

Patrick O'Brien
Managing director | Risk and Financial Advisory | Deloitte Consulting LLP
+1 571 882 6541 | patobrien@deloitte.com

Patrick O'Brien is a managing director with the Defense, National Security and Justice practice at Deloitte.

Anne Marie Kelly
Senior manager | Risk and Financial Advisory | Deloitte Consulting LLP
+1 202-617-1661 | annekelly@deloitte.com

Anne Marie Kelly is a senior manager with Deloitte Advisory LLP in the Forensic & Investigations practice.

The Deloitte Center for Government Insights

William Eggers
Executive director | Deloitte Services LP
+1 571 882 6585 | weggers@deloitte.com

William Eggers is the executive director of Deloitte's Center for Government Insights, where he is responsible for the firm's public sector thought leadership.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Aditi Rao, Blythe Hurley, Abrar Khan, and Nairita Gangopadhyay
Creative: Sonya Vasilieff
Promotion: Alexandra Kawecki
Cover artwork: Sonya Vasilieff

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.