Remarks of Glenn S. Gerstell  
General Counsel, National Security Agency  
as prepared for delivery to the  
Standing Committee on Law and National Security of the American Bar Association  
Washington, DC  
January 15, 2020

Something quite remarkable happened in late December -- yet it went almost unnoticed, buried in what everyone would agree has been an exceptionally heavy news cycle. A Russian Soyuz spacecraft carried two American astronauts to the International Space Station. Since the retirement of the last Space Shuttle in 2011, America has been exclusively dependent on Russia to get our astronauts to and from outer space. We have no operational backup. NASA’s hope is that sometime later this year two private sector companies, Space X and Boeing, will be able to take over the task of launching Americans and certain payloads into space.

Just consider for a moment these fascinating aspects: the most powerful country on Earth, which put a man on the moon, is now dependent on a nation largely regarded as an adversary, one with less than the combined GDP of Illinois and Pennsylvania, while our federal government awaits developments in the private sector. I am simply remarking on this situation, not being critical of it; there are certainly good reasons for shifting some capabilities to the private sector. But putting aside the obvious implications for our space endeavors, which is beyond the scope of my talk today, our reliance on the Soyuz illustrates several factors that have profound implications for our national security.

To take just three of the more obvious factors at play here:

First, unlike industrial development, technological development is less susceptible to or contained by national boundaries. Thus, countries around the world now have the potential to challenge or perhaps surpass America’s technological advances -- so we can no longer take for granted a monopoly or indeed even an overwhelming advantage of national power. Technological capabilities can be relatively quickly built up, whether through dedication of resources or theft of intellectual property, and the very nature of technological development is such that it is possible for one country to leapfrog over another relatively quickly. Technological development doesn’t necessarily require massive natural or capital resources -- so that when central governments such as Russia or China undertake a concerted effort, rapid progress is possible. This has clear strategic implications.

Second, the global nature of technological development and trade produces entanglements and reliance on relationships that aren’t necessarily congruent with national political and strategic goals. Offensive and malicious cyber activity, often unattributable, crosses sovereign boundaries with impunity, making it harder to hold a foreign nation-state accountable for domestic damage. All of this introduces extraordinary complexity into international relations and national security arrangements.

Finally, for a variety of reasons, the balance between the federal government and the private sector in the area of technology is undergoing rapid, significant change. It used to be that the government was unquestionably at the center of technological development. To use our space example, just think back to the early days of
NASA where as a result of the effort to put a man on the moon, everything from computing power to advanced metallurgy was in large part in the hands of federal government. But today, innovation, research and development across the entire the entire field of technology are in many, admittedly not all, respects led by the private sector. Government often lags behind, and relatively speaking, spends a dwindling amount on technological research. The Congressional Research Service estimates that in the period after World War II, the United States accounted for almost 70% of global R&D expenditures; by 2016 that figure dropped to 28% as other nations picked up the pace.

I’d like to explore some of the challenges to national security that arise from these factors. I am doing so from the vantage points of a lawyer and as someone who for almost the past five years has been part of the Intelligence Community’s effort to help keep our country safe against a variety of threats. The latter perspective is clearly relevant, but why is the lawyer viewpoint pertinent? Ultimately, these challenges will present a series of policy choices, and those in turn will require new laws or amendments to existing laws. That of course is why we as attorneys must have a deeper understanding of the problems, so we can help guide policymakers. We could spend the entire afternoon talking about the national security ramifications of the trends I mentioned a minute ago, and still not exhaust the topic. So let me instead focus on just four of the resulting problems or challenges that will be critical for attorneys and policymakers in the national security sector to understand and address.

The first challenge is surely China, an adversary and partner rolled into one. There isn’t a better example of how technology knows no boundaries and how global technological development and trade produce complicated interdependencies. For the first time since the United States became a global power, we must now confront another country that represents not merely a political or military threat -- as was the case in World War II and its aftermath in the Cold War -- but also an existential economic one. Complicating the picture is the fact that China is not simply an adversarial threat. Both China and the United States depend on each other as trading partners. Just as in the case of reliance on Russia’s Soyuz, we need China and we need it to be part of the world order. The days when we faced clearly defined threats in the form of Communism or terrorism are over; we are now in an era of global complexity and interdependencies. But, it is equally true that China has been the perpetrator of perhaps the greatest transfer of wealth in history by stealing intellectual property from our defense industrial base as well as academia and indeed, almost every sector of our economy. That cyber theft enabled China to rapidly rise to threaten not only our economic hegemony but also, at least in certain places around the globe, our military position. From the point of view of our nation’s intelligence agencies, this means that the spectrum of risks and challenges we must uncover, analyze and understand is far greater. Of course, we need to understand the plans and intentions of an adversary on the political and military levels. But the difference now is that national security mandates that we understand the full scope of China’s technological and economic development -- in other words we need not only weapons analysts but also experts in artificial intelligence, metallurgy, biotechnology, quantum computing, crop genetics, port logistics, finance -- in short, almost every facet of economic activity. On its face, this presents a significant challenge for our intelligence community.

Another challenge -- and what is surely the most pernicious effect of the technological revolution -- flows from the global, border-destroying nature of technology and cyber. That is, of course, the advent of cyber maliciousness. It is almost impossible to overstate the gap between the rate at which the cybersecurity threat is getting worse relative to our ability to effectively address it. The simple fact of the matter is that no nation has yet found an effective solution to stop foreign malevolent cyber activity. We will continue to be confronted by this challenge in 2020 as we seek to make sure our national elections are free from foreign cyber interference and influence. Ransomware will probably get worse in type and scope, cyber theft of intellectual property and economic data will continue, and sectors from municipal governments to air transportation to port operations to healthcare will remain vulnerable to cyber wrongdoing. The advent of the Internet of things, 5G telephony and the increasing role of artificial intelligence increases the potential targets and victims of malevolent cyberactivity.
The task for the national security sector is to anticipate cyberthreats, try to stop them where we can and help build a system of resiliency to surmount this problem. But our laws and government structures are not where they need to be to facilitate that task and confront this rapidly mutating threat. That is not to say that a great deal of important work hasn’t already been undertaken, but simply that the threat is advancing at a faster pace. One particularly vexing area for us is dealing with the domestic effects of foreign cyber activity. Heretofore we have relied on our ability to safeguard our national security by dealing with threats beyond our shores exactly where those threats resided. The foreign focus of our intelligence agencies, our four-decade old system of surveillance laws, and the manner in which our First and Fourth Amendments have been interpreted to provide domestic protections, have yielded an overall legal scheme that I doubt anyone would come up with in the face of today’s threats. Yet let me be clear and emphatic that we treasure the rights we have as citizens under that constitutional scheme and I am not suggesting it be diluted in the slightest. The challenge is simply how do we preserve our American values of liberty and freedom while constructing appropriate new government structures and laws to deal with these new threats? This year, Congress and the American public will consider a draft of pending cybersecurity legislation and examine cybersecurity structural recommendations made by the National Infrastructure Advisory Council as well as the forthcoming Cyberspace Solarium Commission report. NSA and the other components of the Intelligence Community will have to determine how they can most effectively participate in and support whatever governmental changes may be on the horizon.

The Soyuz example also highlights how the role of the private sector is changing especially in areas of technological development. And that presents the third challenge to which the national security sector must adapt. The private sector will have more data about individuals and businesses than any government, whether it’s purchasing history, geolocation records, health information or other economic data. The extent to which this puts effective power in the hands of the private sector and the extent to which the private sector is permitted or required to share that information with the government will be a defining public policy question of the next decade.

Government will increasingly rely on the private sector to achieve national security goals, and the private sector will increasingly bear some responsibilities historically borne solely by the public sector. It used to be clear that only government was responsible for national security, and the private sector was largely free to pursue its economic goals. Similarly, it used to be that only governments had the resources and ability to develop instruments of war and the projection of national power. Technology, however, has changed that. Private parties are now capable of causing as much harm as a nation-state. In another change, the private sector is increasingly called upon to protect vital infrastructure, to deploy cyber defenses against foreign mischief, and to furnish information that had previously been the province of government. Consider, for example, the extent of satellite imagery now in private hands and how just a decade or so ago that had been something only governments were capable of. As technology makes national security more of a shared responsibility between government and the private sector, this will increase mutual reliance and introduce complications. And as the private sector assumes more responsibility, the public interest will require greater burdens and scrutiny placed on that sector’s ability to perform, with restrictions on everything from data management to foreign supply chains. In the past year we have seen this issue play out in the effort on the part of the US government to persuade both private sector telecom companies and our foreign allies to eschew Huawei 5G equipment for national security reasons. Actually, Huawei is a powerful example of a complex issue that reflects all of the implications I first mentioned -- rapid technological advances by China, the potential for cyber mischief and complications with global relations and the private sector. The different approaches of our own Five Eyes partners, let alone other allies, clearly illustrates the complicated nature of these technological developments and dependencies.

Finally, the task of our national security agencies in keeping our nation safe will become more difficult not merely because of the challenges and problems I just described, but also because it might be more difficult to
retain the public confidence that those agencies must enjoy in order to be effective. Considering the future world of deep fake videos, spoofing voices and malicious foreign trolls on the internet intent on exploiting existing differences, many worry that we are inexorably on our way to a period of delegitimization and diminution of public trust in institutions. In the national security sector, where protecting the nation often means that very little can be said about the activities of our intelligence agencies, it is critical that whatever information is affirmatively disclosed is believed. Whether it is official denials of action, a statistical report on surveillance, or the results of an investigation undertaken by the executive branch, Congress or some commission, it is crucial that national security actions obtain broad public acceptance.

The ability to obtain that acceptance can be eroded quickly by the intense polarization of the current moment, but of greater and more enduring concern to the national security sector is the pernicious effect of foreign influence campaigns on the internet, which increasingly is the place where most Americans obtain their information. The ability to obfuscate one’s tracks in the cyber domain presents obvious challenges to our national security. Anonymity is the gateway drug to cyber maliciousness. But the rights to privacy, anonymity and unfettered speech can clash with the need to keep our society safe, and our nation will have to attain the right balance, reflecting our core values.

How well we address these four challenges in the next decade -- coping with China, cyber maliciousness, calibrating the balance between the public and private sectors in the national security area and maintaining public confidence in our national security agencies -- will be the defining elements of our nation’s security.

Our intelligence and defense communities have proven themselves adept at meeting complex and significant problems. But these four challenges are unprecedented because of their ubiquity, speed of change and potential for deep injury. True, the specter of nuclear war or terrorist acts inspires greater fear, but in some ways those threats seem more manageable. The very defined nature of those threats permitted a concerted global strategy to effectively address them, and most importantly did not potentially entail significant development of key societal policies. By contrast, these new challenges do not allow for a crisp single strategy to address them, and they may well require substantial changes in the way we think about some important things.

Finally, in laying out these problems, I do not by any means want to suggest we are doomed. I am, however, saying the time to act is now, before these powerful trends make it even more difficult to address the challenges. This will require thoughtful action across the executive branch, Congress, and the private sector.

When I joined the National Security Agency, I had limited prior interaction with the national security and military sectors. Yet now, as I am about to depart almost five years later, the overriding impression I have is that our nation is fortunate to have so many talented men and women who are willing to serve in those sectors. At my own agency, the National Security Agency, our people could make much more money in the private sector, and yet they spend all or a key portion of their careers in government because of their desire for public service. I wish the American public could see for themselves just how true that is, and see how these intelligence community professionals fervently desire to adhere to the law, be non-partisan and help keep our country safe. Having had the privilege of assisting on the front lines in national security efforts, I am confident that we have intellectual ability, moral integrity, skills and dedicated professionals across the intelligence community and defense establishments. In short, I have no doubt that we are capable of addressing these challenges. But it will require a broad and integrated effort to do so and I know that the lawyers in the national security sector, as represented by this ABA committee, can and should be in the vanguard in addressing these challenges.

###

*Please direct inquiries to NSA Public Affairs (443-634-0721; mediarelations@nsa.gov)*