BENS INSIGHTS:
Elevating Thought Leadership in National Security

BUSINESS EXECUTIVES FOR NATIONAL SECURITY
SECURING AMERICA'S FUTURE

Biotechnology's Security Frontier: Navigating Innovation and Safeguards

Navigating Biotechnology Innovation and Safeguards

Biotechnology is rapidly evolving into a critical arena for national security, with innovations that have profound long-term implications already beginning to emerge. As the biotech sector advances, much of this progress is taking place in industry, necessitating proactive public-private collaboration to stay ahead of potential risks. Moreover, the dual-use nature of many biotech advancements, as well as concerns over supply chains and the security of innovation, underscores the urgency of safeguarding these developments. By engaging with industry leaders, policymakers can help prevent misuse and guide biotechnology in ways that bolster national security and public health.

To better understand the intersection of biotechnology and security, BENS recently interviewed industry leaders **Ms. Patrice Bonfiglio**, President of Sarissa Capital Management; **Dr. Ansbert Gadicke**, Managing Director of MPM Capital, Inc.; and **Mr. John Prufeta**, CEO & Managing Partner of Medical Excellence Capital.

Patrice Bonfiglio
President
Sarissa Capital Management

Ansbert Gadicke, M.D.
Managing Director
MPM Capital, Inc.

John Prufeta
CEO & Managing Partner
Medical Excellence Capital

Note: Interviews have been edited for length and clarity. The views expressed are their own and may not reflect those of their employers or BENS.

Why should biotechnology be a key technology in the National Defense Strategy in the next decade? What barriers or opportunities exist for improved collaboration between the biotech industry and the U.S. National Security enterprises?

Patrice Bonfiglio: Short answer--Yes, biotech should be included as a key technology in the National Defense Strategy. Sensitive information is increasingly at risk of exposure to global counterparts, including adversaries. For example, genetic data from U.S. citizens, like that collected by 23andMe and other consumer genetic companies, could be sold to foreign entities. Similarly, the rapid adoption of generative AI raises new security concerns. While most interactions with AI chatbots, like ChatGPT, are harmless, users might input sensitive information into public versions of chatbots, which use that information for training and can become used in responses to other users. The speed at which information is shared and analyzed through generative AI and large language models (LLMs) is staggering. For example, there are a growing number of users that rely on ChatGPT and other chatbots to review medical insurance claims and denials, in order to draft appeal letters and suggest resources. If medical records are uploaded as a part of that process, then medical and genetic data can be distributed from the chatbots to adversaries if given the correct prompt. Since the personalization of biological weaponry is a threat, it becomes key that we defend against it at the same speed that information can be made available to adversaries. This underscores the need for oversight to prevent sensitive data from being exposed or misused.

When we are speaking about barriers to collaboration between biotech companies and the U.S. national security enterprise, we must address a major barrier the biotech industry faces overall. Biotech companies are driving innovation that is both critical to national security and patient lives. The ability for the biotech industry to thrive and collaborate gets stifled when you factor in the power wielded by the pharmacy benefit managers (PBMs). The PBMs are mandated through Medicare to act as an intermediary between the pharmaceutical manufacturers and health plans, but two detrimental outcomes happen. Smaller biotech companies can be excluded from the market if PBMs don't favor their product over therapies from paying higher-paying pharmaceutical companies, and that can happen even if the biotech company has a drug that is more efficacious. So, they can get blocked out of their only market if they are a single product company. Also what can happen is that the PBMs can require rebates so large, that biotech companies end up paying over 100% in rebates, forcing the company to operate at a loss if they want to sell the drug through Medicare.

Politicians are increasingly aware of this, with the potential for bipartisan support to reform PBM influence and open paths for biotech partnerships in sectors like national security. Funding remains a major barrier, as private sector financing alone is insufficient to support these high-potential companies, underscoring the need for broader financial backing to sustain biotech innovation.

Ansbert Gadicke: Biotechnology should be integral to the National Defense Strategy due to the rising risk of lab-generated pandemics and engineered pathogens. A lab-generated virus with a high mortality rate could disrupt society far more severely than COVID-19, affecting essential services and leading to widespread collapse. Unlike nuclear threats, which require significant resources, deadly

viruses can be engineered with accessible equipment, making biotechnology a potentially powerful tool for both national security threats and defense. Incorporating biotechnology into national defense planning can ensure better preparedness against potential biosecurity risks and help mitigate the impact of future biological threats.

Improved collaboration between the biotech industry and U.S. national security is crucial but currently limited. Although many biotech firms would welcome involvement in defense-related biosecurity projects, they often lack the financial means to do so due to limited cash flow and investor interest, especially for pre-commercial companies. Government grants and strategic funding could unlock significant opportunities by enabling biotech companies to prioritize national defense projects and preparedness initiatives. There is also an existing foundation for collaboration, as many biotech advancements are based on NIH-funded intellectual property. With direct support from national security agencies, these companies could integrate their innovations into a comprehensive defense strategy, closing critical gaps in biosecurity preparedness.

John Prufeta: Biotechnology must be a priority in national defense, given its implications for both historical and emerging biological threats. Unlike traditional weapons, biological agents are increasingly affordable and accessible due to advances in computational biology and click chemistry, allowing even smaller actors to develop customized biological threats. This "democratization" of technology poses significant security risks, as illustrated by the COVID-19 pandemic. While the rapid vaccine development highlighted the biotech industry's capabilities, it also underscored the essential role of government support. U.S. investments in mRNA technology, driven by DARPA years prior, demonstrated that effective responses depend on proactive research rather than reactive measures.

Addressing these challenges requires stronger engagement with the scientific community to identify and mitigate biotechnological threats. Currently, there is limited discussion on the intersection of biotechnology and national defense, with few forums devoted to this critical issue. By building partnerships with universities and researchers who are leading innovation in this space, the U.S. can ensure that strategies are informed by the most knowledgeable experts, fostering a proactive and comprehensive defense approach to biotechnological risks that rival those of nuclear threats.

What strategies can the United States adopt to strengthen its competitive position in biotechnology, including approaches to minimize technology and data theft, effectively attract and retain top talent, and mitigate supply chain disruptions?

Patrice Bonfiglio: Many conversations with people in the VC world highlight that top-tier schools outside the Ivy League are often overlooked as pipelines for founders. There's a major opportunity for the private sector to build partnerships with labs at large universities, creating a stronger talent funnel and driving revenue from startups emerging from these labs. Strengthening the biotech community through broader university collaborations is essential.

Minimizing technology and bio-data theft needs to be a priority, but it often isn't adequately addressed in the early stages of biotech companies. Cybersecurity is often not fully integrated when a company is first formed. Establishing a required cybersecurity framework could help, and raising awareness

about data theft risks would encourage companies to take stronger precautions. More affordable cybersecurity programs would also make it easier for startups to adopt better practices. Additionally, many companies already use software like Microsoft, which includes built-in data loss prevention tools that can be leveraged to improve data tracking.

Another approach to enhancing collaboration would be to streamline the clinical trial process in the U.S. While there are some efforts are underway, like the FDA's Streamlined Trails Embedded in Clinical Practice (STEP) initiative, we still have to see if the implementation will lead to a true streamlining of the process. If this is the case, then perhaps we can keep more clinical trials in the US, instead of Poland for example, which has 30%-50% less costs while still being influenced by the European Union's regulatory framework. If we can keep more clinical trials here, it would benefit the U.S. in the long run, especially if we want to protect our information within the country.

Ansbert Gadicke: U.S. leadership in biotech is rapidly being challenged by Chinese companies, which benefit from lower regulatory barriers and cost advantages, allowing them to move faster in drug development. A critical issue threatening U.S. competitiveness is data theft; several incidents, such as breaches involving WuXi Biotech, underscore the vulnerability of U.S. firms to intellectual property theft. Many U.S. biotech companies lack the resources to implement robust cybersecurity measures, making government support for industry-wide cybersecurity initiatives essential. A more collaborative approach between the government and industry could help small companies protect their data and retain their technological edge.

Attracting and retaining top talent is also vital for sustaining U.S. biotech leadership, and supportive tax policies play a role here. Stock options are the main tool smaller biotech firms use to compete with larger pharmaceutical companies for talent, but proposals to tax unrealized capital gains could create severe financial burdens on employees without actual income to offset them. If implemented, such policies could make it harder for U.S. biotech firms to attract talent. While training is essential, companies are already doing an effective job internally, with limited government intervention needed.

In terms of supply chains, the biotech industry faces fewer challenges compared to sectors like semiconductors. While some U.S. companies work with Chinese suppliers for cost reasons, similar resources are available domestically and in Europe, though often at a higher price. Maintaining diverse supplier options within allied countries could further secure the supply chain. With a strategic focus on cybersecurity, favorable tax policies for talent retention, and a diversified supply base, the U.S. can solidify its competitive position in biotech despite rising international competition.

John Prufeta: To strengthen its competitive position in biotechnology, the United States should prioritize domestic production capabilities and reduce reliance on foreign suppliers, especially China, which heavily subsidizes biotech manufacturing. By implementing supportive policies that incentivize U.S.-based production of essential biotechnological components, the government can help offset the cost advantages currently held by foreign competitors. This strategy also includes addressing pricing policies to reduce the financial burden on American consumers; adjusting international drug pricing could ease costs domestically without sacrificing global competitiveness. At the same time, incentivizing American companies to prioritize local sourcing over cheaper but riskier foreign options will mitigate potential supply chain vulnerabilities.

Attracting and retaining top talent in the biotech field is another priority that requires a dual approach of educational investment and immigration policy. Increasing STEM-focused educational programs, especially in biotechnology, will create a stronger domestic talent pipeline, but the U.S. should also continue to attract international talent by streamlining pathways for skilled workers to contribute long-term. Addressing data and technology theft, especially from China, requires robust policy and enforcement measures, including strict protections on trade secrets and increased surveillance of sensitive research environments. By strengthening cybersecurity standards, penalizing theft, and implementing strategic oversight of sensitive areas, the U.S. can protect its competitive edge and innovation output in biotechnology.

How significant do you believe the risks are related to the adversarial use of biotechnology? What might the U.S. do to address these risks better as they relate to threats from state and non-state actors?

Patrice Bonfiglio: For me, it's less about the likelihood of something happening and more about how easily it could be done—that's what's truly alarming. If something is easy enough to accomplish and could have a huge negative impact, we need to be prepared from that standpoint. I wouldn't risk sidelining the threat. My focus is usually on countries like China or Russia, but it's eye-opening to realize that threats could come from multiple directions.

This ties into the supply chain issue. We're reliant on other countries for ingredients, certain capsules, and animal testing from companies like WuXi. The amount of non-U.S. intervention in our supply chain exposes us to vulnerabilities. If the government had a system—perhaps activated only in times of heightened threat—to produce essential products domestically, it would be invaluable. Take antibiotics as an example; we can't manufacture penicillin in the U.S. anymore, a capability lost years ago. In a biological warfare scenario, having the infrastructure to produce critical medicines domestically could be essential to saving lives. 'How prepared are we', is a question we should never stop asking.

Ansbert Gadicke: The risks of adversarial use of biotechnology are highly significant, given how accessible and unregulated the tools for engineering pathogens have become. A single individual with basic virology knowledge and equipment readily available online could create a virus with serious public health implications, posing a real threat from both state and non-state actors. This ease of access, coupled with the widespread availability of viral genetic sequences, means that preventing malicious use is nearly impossible. The U.S. must take these risks seriously, as the low barriers to entry make it likely that adversarial biotechnology could emerge as a substantial security threat.

To address these risks, the U.S. should prioritize government support for biotech collaboration focused on biosecurity and rapid response capabilities. Investment in partnerships with biotech firms developing cutting-edge vaccine and antiviral technologies could enable quicker responses to future threats. Government funding would allow for preparedness programs, including the development and stockpiling of antivirals, which would be essential to manage outbreaks before vaccines can be distributed. Such an approach could significantly improve the country's response readiness without relying solely on private sector investment, which may lack the long-term focus necessary for biosecurity.

John Prufeta: The primary concern in biotechnology isn't so much that major state actors like

Russia or China will develop a novel bioweapon, as any aggressive deployment of such technology would provoke a formidable response from our defense capabilities. Rather, the more immediate risk lies in the increasing miniaturization and accessibility of biotech and chemical technologies, which dramatically lowers the barrier for non-state actors. With relatively modest funding, smaller hostile groups, including splinter groups within allied democratic nations, could carry out potentially devastating actions. This scenario mirrors nuclear proliferation but is far more accessible, making it an urgent issue. Organizations like BENS are pivotal to countering these emerging threats; they bring together experts and leaders across sectors to address critical security gaps, prioritize pressing questions, and deliver the strategic feedback necessary to bolster national defenses in this evolving landscape.

1030 15th St. NW · Suite 200 East
Washington, DC 20005
www.BENS.org | X: @BENS_org | 202.296.2125