

**Comments to the Blue Ribbon Study Panel on Biodefense**  
**Kenneth Luongo**  
**President, Partnership for Global Security**

**Hudson Institute, Washington D.C.**  
**April 25, 2018**

Chairmen Lieberman and Ridge and distinguished members of the panel, thank you for the invitation to provide comments to you on Transnational Biological Threats and Global Security.

I agree completely with the first sentence of the Preface of your October 2015 report – “The United States is underprepared for biological threats.” Despite your excellent analysis and recommendations we remain underprepared while some of the dangers and challenges have continued to develop and grow in intensity.

I am going to focus my remarks on four key issues:

- Infectious Disease and Pandemics
- Emerging Technologies
- International Threat Reduction
- International Institutions

**Infectious Disease and Pandemics**

Infectious disease and pandemics are the clearest and most immediate danger we face from biological threats. Yet, this challenge is primarily treated as a medical issue not a global security issue. And, within the medical community it is not at all clear that we are ready to effectively deal with the consequences of a severe infectious disease outbreak or pandemic.

Just earlier this year we saw some hospitals where severe flu had taken hold stretched to their limit. In Rhode Island, hospitals diverted ambulances because they were flooded with patients. In San Diego, one hospital erected tents outside the emergency room to manage flu patients. And, this is an infectious disease that the country prepares for every year.

What does this anecdotal evidence tell us about the preparedness to effectively manage another bout of bird flu or swine flu? Or emerging pathogens for which few, or no, medical countermeasures exist - the WHO includes in this list Ebola, MERS, and SARS among others.

There are several contributing factors to this situation. One is the increasing urbanization of the global population and the stresses that a potential outbreak would place on urban hospitals.

Another is the decline in anti-viral and antibiotic research and development. The U.S. launched a National Action Plan for Combatting Antibiotic-Resistant Bacteria in 2015. This included the creation of a biopharmaceutical incubator to promote innovation and increase the number of antibiotics in the drug-development pipeline. But, it has a hazy timeline, and in the meantime, no new class of antibiotics has been discovered since 1987. Antibiotic resistant diseases are

growing. It is estimated that the global death toll from drug-resistant infections is several hundred thousand people annually. That could reach into the millions by mid-century. This is primarily impacting developing countries, but it could spread.

Third, there needs to be better and more focused attention on modelling the potential for the spread of disease. While some work on this is being done and contemplated inside governments, it is not very effective or comprehensive at the moment.

Finally, today, almost 75 percent of all new, emerging, or re-emerging diseases are zoonotic in origin. In our highly interconnected world, infectious diseases can spread quickly and far in a short period of time. The SARS, H5N1 avian influenza outbreak, and the H1N1 influenza pandemic are clear examples of how dangerous diseases can quickly spread and create serious response challenges.

## **Emerging Technologies**

Compounding the infectious disease challenge is the rapid advance in technology.

Advances in biotechnology, nanotechnology and related disciplines pose a significant dilemma. They promise benefits for human health yet can be misused for hostile purposes.

The field of synthetic biology, in particular, offers a number of challenges. It combines chemical synthesis of DNA with genomics to enable the rapid manufacture of DNA sequences or the assembly of them into new genomes. From a risk perspective, the ability exists to create new biological systems and organisms that can be used for malicious purposes, including defeating existing immune defense mechanisms.

Much of this field in democratic countries is managed by the private sector and in authoritarian nations by the government. But, in both areas, there is little transparency in synthetic biology. This raises questions about what is going on in the laboratory and how governments with control over the technology may be managing it – and for what ends.

Major biotech countries including the U.S. and those in the E.U. have national frameworks and legal requirements governing biosafety and biosecurity. However, the governance of activities in other major biotech countries, like China and Russia, are more opaque.

There also are few global rules governing synthetic biology activities. The Biological Weapons Convention bans biological weapons, but has no enforcement mechanism. The Australia Group is an informal association of over 40 nations that formed a synthetic biology advisory body in 2008.

There is a synthetic biology Code of Conduct that outlines best practices. It was driven by concerns that genetic technologies could be used for bioterrorism or as a biological warfare agent. While adherence is voluntary, a value of the Code is that it requires gene synthesis providers to screen genetic sequences ordered by customers against a database of known pathogenicity or virulence factors and to screen clients to determine their legitimacy.

While the governance process seeks to catch up with the rapid trajectory of biotechnology, the industry is undergoing additional changes. Biotech is being significantly impacted by digital advances including data processing and artificial intelligence, and by nanotechnology. In the U.S., the Defense Advanced Research Projects Agency is looking at how synthetic biology can lead to advanced nanotechnology through a program called “Living Foundries.”

The goal is to standardize and streamline genetic engineering so that it can more easily and cheaply provide new materials, capabilities, fuels and medicines - in a Lego-like fashion that can create biological mini-machines. While this may benefit the bio-products needs of the U.S. military, it may also be replicated by hostile nations.

As long as biosecurity regulation and oversight remain national and globally uneven, the world will face greater bio-vulnerability. As life science continues to advance, more transparency and oversight will become more important.

### **International Threat Reduction**

One way that the U.S. and its allies have attempted to increase the transparency and insight into biological activities in locations of concern has been through its threat reduction efforts. There are several efforts, including in the Departments of Defense and State, some of which have their origins in the ground-breaking Nunn-Lugar program. But those programs have changed missions over the years as collaboration in Russia and the FSU shut down and other opportunities opened up.

DoD’s Cooperative Biological Engagement program is focused on addressing global health security threats by working with partner nations to improve biosafety, biosecurity, and support disease surveillance for traditional select agents and emerging pathogens. State is involved with the Australia Group, the BWC, and has supported U.S. efforts to curb the Ebola epidemic.

In 2014, the Global Health Security Agenda was launched as an international partnership with governments, international organizations and non-governmental organization. The goals was to strengthen the barriers against infectious disease and elevate global health security as a priority issue. The U.S. and a number of its European and Asian allies are members as is China. But Russia is not a member.

These efforts are all worthwhile and important but they have left many dark corners of the bio world unlit. It then falls to the intelligence community to determine what activities are occurring in key countries like Russia, Syria and North Korea. But, bio laboratories are small and difficult to monitor remotely and there is little of the large infrastructure, equipment, and signatures that are associated with a nuclear program for example. And, historically, the amount of intelligence community person-power that has been devoted to bio threats has been small.

There also are challenges posed by non-state actors including terrorists. State supplied bio-weapons to terrorists is one pathway of concern. But, there is a growing DIYbio community that has developed that includes hobbyists and after-hours professionals. This is a highly dispersed

community that is essentially unregulated. The threat spectrum in this area includes accidental exposure, deliberate exposure, and dissemination of information. The National Science Advisory Board for Biosecurity made some useful recommendations for how to manage the DIY phenomenon in 2011. However, terrorists have become more brutal and are better resourced than in the past. Western intelligence agencies have stated that the Islamic State has been trying to develop biological weapons at its bases in Iraq and Syria. Syria, itself is suspected of maintaining a biological weapon program and in explaining the most recent attack on Syrian facilities, senior Pentagon leaders noted that one of the targeted scientific facilities was engaged in biological research. Given these comments, the unbridled use of chemical weapons by the Syrian government, the covert effort to construct a nuclear reactor, and their close relationship with North Korea, we should be very wary of, and alert to, any potential bio weapons activities in Syria.

Further, the Department of Homeland Security must remain vigilant about the potential for a potential bio attack on the U.S. through its BioWatch program and other activities.

But, overall, it is clear that given the myriad international challenges that the U.S. government has to deal with on a daily basis and the lack of a bio-weapons attack by terrorists, we have lowered the priority of this threat in the country. That is a mistake.

### **International Institutions and Governance**

As the Panel has made clear in its earlier report, the U.S. government desperately needs to get better organized on addressing and preventing the bio threat than it has been able to do so far.

But, the report also made the same point about the international community. It said, “Global prevention and response capability will not come from the WHO; it must come from nations that agree to make it a priority.” There were then recommendations for private-public partnerships that could improve the international response to a large-scale outbreak.

Beyond, the logistics, there is also a lack of harmonized and globalized regulatory and governance system. And, a disjointed reporting and surveillance system for infectious disease hot spots. Also, the International Health Regulations remain voluntary with inadequate funding for broad implementation.

In my work in nuclear, bio, and other transnational security areas I have found that the challenges in the bio area are similar to those in other areas. The disconnect between governments and the private sector stakeholders; the inability to coordinate effectively by breaking through silos rather than building them higher; and the cross cutting nature of the challenge – affecting the economy, security, health, and human well-being – are elements present in all of these transnational security areas.

My recommendation is that we should work through the challenges in each area while also working to find a model that can be applied across them all.

Thank you.