In Our Own Way? – What National Security Must Learn from the Pandemic

In the months since the Covid-19 pandemic shook the country and the world, there has undoubtedly been a steep learning curve on how to protect Americans from illness and economic loss. When it came to national security, sick troops and stretched resources challenged the military's readiness. This pandemic, however, cannot be viewed as an isolated, once in a lifetime crisis, but should solidify some pivotal realities for national security leaders and practitioners.

The biggest threats don't have flags or faces

From the Revolutionary War to the Cold War to the War on Drugs, the American mindset has traditionally been on naming the enemy and going to battle. That may have worked in the past, but the enemy-based mentality often mischaracterizes the threats today. Great Power Competition, for example, is a race of hardware, investment, and planning. And the Cold War already proved that the race to mutually assured destruction was is no one's best interest and very expensive to maintain. During the War on Terror, risks posed by smaller states and non-state actors revealed cross-national threats, such as religious fundamentalism, nuclear capabilities, and cyberattacks. The Covid-19 pandemic has proven that the most destructive threats, particularly existential ones, are intangible, unpredictable, and marginalized. Despite the known dangers of, and preparedness against biological weapons or outbreaks, Covid-19 has already claimed double the number of lives than Americans killed in all wars since World War II. Last month, a ransomware attack linked to a Russian cybercrime group, shut down the entire computer network (impacting patient data, laboratory systems, and clinical information) of a large hospital system with more than 400 locations across the country. Some critics dispute the severity and even existence of climate change, but looking ahead, environmental issues are poised to exacerbate food and water insecurity, migration trends, and impact global industries, advancing slowly to desperate battles over basic resources. Whether it's from a lack of imagination, preparedness, or cohesive action, national security needs to focus less on vilifying a 'who' and more on 'what' can actually damage and destroy America and her allies.

Innovation isn't just technology

The Covid-19 pandemic demonstrated once again that necessity is the mother of all invention, and that invention isn't necessarily technological. Quarantines made working from home a reality for more Americans than ever. In the past, many organizations would not trust or imagine employees to be productive outside of a traditional office setting, but the new normal of remote and alternative workspaces has quashed most of those fears across the public and private sectors. While enabled by existing telecommunications and technologies, the innovations were that of people, processes, and perspectives. Mitigating and adjusting to the crisis meant pivoting skills, resources, and locations, not large-scale strategies. For example, battling the virus meant changing gears on the production and distribution of personal protective and medical equipment, and using existing platforms to share and develop medical knowledge. Likewise, across national security organizations, the need for innovation had been paramount in information sharing, acquisitions, and personnel development. In fact, modernization of government and military systems have been driven by eliminating an overabundance of legacy applications and simplifying processes, and not by reinventing the wheel. It's understandably easy to get distracted by the new and shiny, such as building a new weapon to outperform another weapon. After all, national security is increasingly discussed in terms of ‘quantum computing,’ ‘swarming technology,’ and ‘unmanned-unmanned teaming.’ As much as cutting-edge technology is required for the future battlespace, the battles are still conducted by people. Every artificial intelligence tool and unmanned technology is designed by and utilized to serve human intentions. While IEDs and drones are no match for missiles or air power, simpler technologies and imagination proved rather destructive and disruptive in recent operations.

Innovation also applies to how we think about national security. For example, a recent assessment by the House Intelligence Committee found that the U.S. intelligence community “will be hard-pressed to meet China’s multidimensional challenge if it stays in a counterterrorism mindset” and must become “more adept at analyzing nonmilitary threats, such as health, the economy, and climate change.”[1] Even the significant shift to multi-domain operations, such as the Joint All Domain Command and Control (JADC2) concept, is outpaced by Russia, who has pursued hybrid warfare for some time; leveraging the conventional and irregular with the political and information. While recent JADC2 exercises enabled ubiquitous domain data exchanges to shorten sensor-to-shooter time, Russian exercises this summer focused on multi-sphere operations conducted over 400 tactical episodes simulating hostilities in various environments and space within the framework of a single operational background in real time. As the character of war evolves, those who prevail will master the lethal combination of new ideas, operational concepts, and solutions, not just the technologies.

There’s always a war at home

Nearly every war or military action with which the U.S. has been involved has faced a battle for the hearts and minds at home, from Loyalists in the American Revolution to contemporary anti-war protests. The Covid-19 pandemic, however, has been part of a growing trend of the American public misunderstanding the threat altogether. How can Americans be protected from a pandemic if they don’t understand or believe the threat even exists? What happens when they amplify the threat’s severity by refusing safeguards and creating alternative conspiracies? The lessons should have already been heeded. The September 11th attacks led to numerous attacks against Muslims and people of color assumed to be Muslim, as well as conspiracy theories that pointed the finger at the U.S. itself. Information warfare has been increasingly effective here, as well, including the Chinese government’s offensive shaping of the pandemic narrative to Russian trolls and bots encouraging contrarian beliefs and actions. As unimaginable as it may be, going forward, national security approaches cannot neglect the battle for the truth, especially at home. Just as threats and tools evolve, so must be the way they are seen. The Covid-19 pandemic has raised many challenges but taught many lessons that those entrusted with protecting the nation must learn or risk getting in their own way.

[1] Amy McKinnon, “U.S. at Risk of Being Outpaced by China, a New Intel Committee Report Finds,” *Foreign Policy*, September 30, 2020, https://foreignpolicy.com/2020/09/30/united-states-risk-outpaced-falling-behind-china-new-house-intelligence-committee-report-finds/