Top Three Things DHS Should Consider Regarding the Laptop Ban

David Inserra

In March, the Department of Homeland Security (DHS) banned electronics larger than smartphones from being carried onto aircraft leaving for the U.S. The ban applied to flights originating from 10 airports in the Middle East and North Africa, although DHS has been considering expanding this ban to include flights from Europe to the U.S.[1] DHS has cited credible intelligence of a threat from explosives being smuggled onto aircraft.

Many policymakers in the U.S. are wondering whether the so-called laptop ban is the correct solution to the newest threat to aviation security. Classified intelligence is essential to answering this quandary, but so are proper risk-management and cost–benefit frameworks. DHS must also consider what alternatives might be implemented to improve aviation security. Should DHS proceed with a laptop ban, it must consider how it can lessen the impact of a ban on travelers in the short and medium terms while looking for longer-term solutions that would allow the ban to be lifted.

The following are the top three things that DHS should consider when making policy in this area:

Consider the Cost–Benefit Risk Analysis. Any policies or combinations of policies that the U.S. adopts should be driven by a careful assessment of risk, how well the proposed policies will address that risk, and at what cost.[2] Policies that improve our security slightly but at immense cost should not be adopted.

In the past, U.S. policymakers have ignored such analysis, and the result has been policies that are difficult or impossible to implement. For example, the 9/11 Commission Act of 2007 required foreign seaports to scan and image 100 percent of the cargo entering the U.S.—despite the fact that the technology, infrastructure, and funding to do so did not (and still do not) exist and that it would cripple global trade. Given such difficulties, DHS still does not require all cargo to be scanned and imaged at foreign ports; instead, it images and scans high-risk cargo (about 5 percent) while scanning nearly all cargo only at radiation portals set up at U.S. ports.[3]

Although new mandates and bans may provide some security, the cost of implementation and its effect on legitimate trade and travel must be considered. If the benefit of such a policy—i.e., a significant reduction in serious risk to the U.S.—is greater than the cost, then that policy should be considered a viable solution.

Seek Out Alternatives. Without knowing the specifics of the DHS intelligence, it is impossible to determine precisely what types of security are needed. That said, the problem at hand is the smuggling of explosives onto aircraft by disguising them in large electronic devices. One obvious alternative is to expand the ban, excluding large devices from planes entirely or applying the ban to all parts of the world, as this would increase security. However, the costs to travelers would be much larger than the limited ban on bringing electronics into the cabin.

On the other hand, there are options that do not involve a ban on devices but attempt instead to reduce risk and improve security in other ways. To better detect bombs, the U.S. could look to deploy additional bomb-detection capabilities. Bomb-sniffing dogs are exceptionally valuable because of their ability to detect explosives in a variety of situations and to do so more quickly than is possible with most of the bomb-detection technologies that are currently available. It takes a significant amount of time, however, to train a dog before it is ready to serve, which makes this a mid-term to long-term solution.[4]

Until more dogs could be brought online, either animals would have to be borrowed from other law enforcement tasks or airport security would have to rely on bomb-detection equipment. While slower than dogs, many bomb-detection devices that have been developed by the private sector can be deployed quickly. The number of dogs or devices needed would depend on the number of terminals or gates to be serviced and U.S. cost–benefit analysis and risk tolerance.

Beyond bomb detection, the U.S. could push for different security checkpoint procedures or policies. Screened U.S. trusted travelers could be generally exempted from extra explosives detection in order to lessen the cost and time of such efforts. Such a change could expand trusted-traveler enrollment, benefiting security and efficiency elsewhere in the travelling process, including the TSA PreCheck line and the Global Entry kiosk when entering the U.S. from abroad. Expanding the benefits of and enrollment in such programs would also require the U.S. to ensure that trusted travelers are subject to proper and recurrent vetting in order to make sure that they remain a lower-risk population.

In general, the U.S. could require more scrutiny at security checkpoints for individuals with electronics. Reportedly, the TSA is already looking at screening changes within the U.S. (e.g., requiring that all electronics larger than a cell phone be placed separately in bins).[5] Specific lanes could be set aside for individuals with such electronics, or there could be extra checks at the gate of an aircraft heading to the U.S. Individuals bringing their devices on board could also be required to turn on the devices, as placing a bomb inside the device often renders the device inoperable.

All of these solutions would cost more money and would likely slow down the security process, but they would likely cost less than a ban. Only DHS can run each of these alternatives through the cost–benefit framework described above to determine how well each solution would mitigate the threat and whether it would be worth the cost.

Mitigate Harmful Side Effects and Pursue Long-Term Solutions. Whatever solution or set of solutions is chosen, there will be side effects and costs. DHS should work to lessen these costs wherever possible. For example, if a ban is implemented, credentialed members of DHS trusted-traveler programs might be allowed to travel with their devices. If the cost of bomb-detection equipment is too high to apply to everyone passing through security checkpoints at airports, such equipment could be limited to specific terminals, checkpoints, or gates where U.S.-bound flights are located.

1. Some news reports say that DHS has tabled the ban, while others suggest that it is still under consideration. Whatever the current state of play, this issue and the recommendations in this *Issue Brief* remain worthy of consideration. Robert Schroeder, "Homeland Security Calls U.S.-EU Laptop Ban Story 'Absolutely Wrong,'" Fox Business, May 30, 2017, http://www.foxbusiness.com/markets/2017/05/30/homeland-security-calls-us-eu-laptop-ban-story-absolutely-wrong.html (accessed June 1, 2017).

2. For additional detail on what such a cost-benefit risk analysis should include, see David Inserra, "Considering the Laptop Ban: Risks, Costs, Benefits, and Alternatives," Heritage Foundation *Issue Brief* No. 4710, June 1, 2017, https://www.heritage.org/homeland-security/report/considering-the-laptop-ban-risks-costs-benefits-and-alternatives.

3. David Inserra, "Congress Must Re-Set Department of Homeland Security Priorities: American Lives Depend on It," Heritage Foundation *Special Report* No. 175, January 3, 2017, http://www.heritage.org/homeland-security/report/congress-must-re-set-department-homeland-security-priorities-american.

4. Most dogs will be chosen when they are one to two years old, often after participating in various behavioral and environmental training programs, and will undergo two to six months of bomb-detection training. See Catherine Savoia, "12 Fun Facts About Bomb Dogs," *MSA Security*, June 25, 2015, http://www.msasecurity.net/security-and-counterterrorism-blog/12-fun-facts-about-bomb-dogs (accessed May 30, 2017), and Ron Nixon, "T.S.A. Trains Dogs to Stay One Sniff Ahead of Bomb Makers," *The New York Times*, May 31, 2016, https://www.nytimes.com/2016/06/01/us/tsa-trains-dogs-to-stay-one-sniff-ahead-of-bomb-makers.html?_r=0 (accessed May 30, 2017).

5. Scott McCartney, "Get Ready to Unpack for Airport Security," *The Wall Street Journal*, May 24, 2017, https://www.wsj.com/articles/get-ready-to-unpack-for-airport-security-1495640411 (accessed May 26, 2017).

Furthermore, whatever solutions are used, the U.S. should look for long-term solutions that provide security at a reasonable cost with minimal impact on legitimate travel. DHS should be seeking the most effective solution, whether it is bomb-sniffing dogs; the development of new bomb-detection, anti-tamper, or X-ray technologies; or something yet unconsidered.

The Ceaseless Search for Security

Few of the numerous risks that the U.S. faces can be completely eliminated, and many will change over time. Such is the case with explosives being smuggled aboard an aircraft. DHS must remain vigilant to head off emerging threats but must do so in a way that protects legitimate trade and travel. By using cost–benefit and risk analysis, seeking alternative solutions, and minimizing short-term and long-term side effects, DHS can advance both U.S. security and economic vitality.

—David Inserra is a Policy Analyst for Homeland Security and Cybersecurity in the Douglas and Sarah Allison Center for Foreign Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.