CHANGE TO REFERENCE OTHER PAPERS WHERE NEEDED/RELIED UPON

Reducing the risks posed to American civilian computer systems by connected technologies and systems – as described in the first article of this series – will require more than one entity taking action. As mentioned in the second article, even international governments taking cooperative steps towards establishing cyber norms and promoting information sharing among allies will only do so much to mitigate the threats posed to civilian networks – including American civilian networks. More is needed. To that end, all levels of government and industry will need to work with each other and with other partners such as universities and research and development centers. These partnerships can utilize industry subject matter experts to better understand the technologies and capabilities that companies have at their disposal. Government specialists can serve as information hubs which collect and disseminate information on industry threats and best practices. Moreover, the government is capable of implementing a wider range of deterrent and response actions to include prosecuting cyber criminals and imposing economic sanctions. Rather than being mired in responding to incidents as they occur, research and development centers are excellent resources to consider long-term, big idea problems and solutions. It is only with largescale, coordinated action that the daunting scope of the threats discussed in this series can be addressed.

There has been some recognition within the United States of the need for such coordinated action to address these threats. For example, Congress established a Cyberspace Solarium Commission in its National Defense Authorization Act for the fiscal year 2019. The Commission includes stakeholders from government, the private sector, and academia and has achieved some success in spurring action. Yet the Commission is far from enough. In the time since the Commission has been created, new and pressing issues have continued to arise at a pace that it cannot keep apace of. From building out the nation's 5G networks securely to continuously improving responses to data breaches of private and public sector organizations, more robust coordinated action is needed. One shortcoming of the Commission is its inability to *require* changes. The recommendations made by the Commission are just that, recommendations. Government agencies, like the Cyber Security and Infrastructure Security Agency ("CISA"), are tasked with securing the nation's cyber infrastructure but are also largely limited to recommending changes to private organizations. Requiring specific action is likely untenable given the myriad organizations and their diverse capabilities; however, providing additional resources to aid organizations looking to improve their security coupled with increasing the liability for poor security practices could provide a working "carrot and stick" method of raising the baseline security posture of the nation's civilian cyber infrastructure.

Private companies enacting change at an organizational level will help reduce cyber risk but increasing individual knowledge of these risks and how to mitigate them is also necessary. Cybersecurity training programs within companies are one method to improve each organization's security within specific systems while likely offering some benefit to individuals in their personal lives. Funding for education programs for K-12 students will help improve cyber literacy generally and provide a higher baseline from which to continue risk mitigation education. Additional funding to universities for cybersecurity education, even as a general education course for various majors would help improve the national risk posture. The funding could also result in filling the millions of open cybersecurity roles and providing additional resources for research. Providing additional resources for research and development might help get the nation out from behind the curve and able to better anticipate coming challenges.

CHANGE TO REFERENCE OTHER PAPERS WHERE NEEDED/RELIED UPON

Improved cyber literacy might also increase the government's ability to keep pace of technological challenges rather than relying on laws created decades ago with few updates provided over that time.

Building public-private partnerships helps maximize the utility of the country's cybersecurity knowledge and expertise. Collaboration across the national landscape not only provides a diversity of thought, it also builds a sense of engagement. By investing time and resources into cooperative agreements and projects, each party will have a better sense of how the outcome will affect them and be able to provide valuable input into the effort. Reducing the risks posed to American civilian computer systems by connected technologies and systems is not a project that can be accomplished alone; it will require nationwide – and international – input and cooperation.