The Internet is a global network of interconnected devices. As such, reducing risks posed to American civilian computer systems by connected technologies and systems will require international agreements in addition to any national efforts. It would be naïve to suggest that all nations will agree to simply cease the use of cyber weapons and deter individual actors from operating across borders. Yet there are some areas where improvements are possible and where international cooperation can be achieved. Successful international alliances, like NATO, have incorporated cyber defense into their understanding of collective defense. The United States also has extradition agreements which allow criminals, including cyber criminals, to face justice in the jurisdiction where their crimes were committed. These steps are necessary to America's cyber risk reduction efforts, but they are not sufficient.

While collective defense agreements can deter nation-state cyber-attacks, the rapidly evolving landscape of information security makes it very difficult to not only attribute who has taken what action – a prerequisite to lawful self-defense – but also to define what even is a cyber-attack. Data exfiltration, reconnaissance efforts, even destructive malicious acts are relatively routine and are generally not considered acts worthy of an armed response. These acts though do not take place in a vacuum; a ransomware attack on a hospital might lead to death or data exfiltration and publication could be seen as interfering with a state's internal governing. Different governments and leadership personalities may make a substantially similar act in one country result in a wholly different response. While this is somewhat true with traditional arms as well, and countries have certainly manufactured reasons to attack, there are still laws that prohibit these actions. These prohibitions create a deterrent, but also allow a range of retaliatory action from non-involved nations to punish the wrongdoer. Calls for international agreement on a set of similar rules in cyberspace are not new, but the problem is likely to only worsen without some established rules.

International Agreements govern nation state action and, in many instances, malicious cyber acts come from sub-state actors. While proxy groups for nations can be dealt with under the umbrella of state action, unaffiliated groups such as terrorist organizations and criminal syndicates pose a more difficult agreement. Unaffiliated groups are rarely parties to international agreements and, even in situations where such groups might be involved, not all malicious groups would be covered. These groups pose additional difficulties in that they operate from countries that may simply ignore the problem or are unable to respond to the issues themselves. Extradition and law enforcement assistance provide some help in resolving these issues, as does coordinated law enforcement action. More, however, is needed to reduce risk to an acceptable level for American civilian computer systems.

Countries should consider international agreements that promote cyber resilience by sharing best risk reduction practices. International trade agreements could also be used as a tool to improve information security by offering lower tariffs to goods that meet an established baseline. Given the shortage of information security professionals nationally and globally, the assessment of new goods might be left to a trusted international organization. By lowering tariffs in this manner countries will not only reduce the price of secure hardware for consumers, but manufacturers of these products will also have an incentive to spend more on secure designs now rather than face higher tariffs down the road. Secure software is more difficult to incentivize via tariffs given online availability, however, countries can promote visa expeditions for software security

positions. Moreover, to reduce the risk of malicious personnel, governments might consider mandating security checks for sensitive positions being filled by foreign actors. As this will impose a cost on the security investigator, government financed investigations or other financial offsets can be implemented to reduce any added burden.

Information sharing agreements can also be used between trusted partners to alert parties of newly discovered vulnerabilities. Though this has limited application to scenarios where the vulnerabilities are not publicly exposed, additional cooperation will reinforce or build trust. These information sharing agreements can also be used among trusted partners to help with attributions for malicious acts by building a shared library of cyber incidents and known actor information. This would allow faster, more certain attribution and therefore improved responses. The library may also assist stakeholders to build more resilient systems.

A strictly national solution to this international problem is unlikely to adequately reduce the risks the United States faces. While international agreement can take some time to build, by working towards these ends now, nations will be better equipped to address the problems of today and tomorrow. By focusing on reducing the risks posed by a multitude of actor types, countries can better protect not only their national security but also that of their civilian computer systems. Working with our partners and allies, while also building international agreement on norms of behavior, is a critical component to securing connected American civilian computer systems.