every day, U.S. military and civilian networks are probed thousands of times for cyber weaknesses. As a result of the mounting threat, there is a growing consensus that international action is required to reduce the threat of cyber war. The U.S. should take the lead in deterring cyber war by hosting a cybersecurity summit—a key first step to building an international cyber accord.

THE THREAT

The growing potential for crippling attacks against the military, utilities, and private networks.

The White House, before dawn: the President is awakened by his homeland security advisor and told that a successful cyber attack on the U.S. has disrupted large swaths of the electrical grid. Later that morning, the Secretary of Defense alerts the White House that the Pentagon’s classified computer systems have been infected with malicious code that has transferred sensitive military information abroad. Within hours, reports come in from banks around the country that financial data have been corrupted. Commercial communications networks are the next to be attacked, and mobile phones across the country stop working. Wall Street trading is halted as stock prices plummet. The U.S. is under attack. A cyber Pearl Harbor has been successfully launched. Not a single shot has been fired or bomb exploded, but America is technologically crippled and its economy is immediately brought to the brink of disaster. The entire nation is confused and fearful of what might come next.

How realistic is such a scenario?

While the elements of this worst-case scenario may be unlikely to happen simultaneously, each type of attack described has already taken place somewhere around the globe. In 2007, cyber attackers used over one million computers operating in 70 countries to launch a full-scale cyber attack against
Estonia, temporarily bringing down the country’s computer networks, including banking and government systems. In 2008, cyber attackers used a cyber-supported kinetic attack against Georgia’s communication systems to hinder the country’s ability to respond to a military attack. That same year, a foreign intelligence agency placed a malicious computer code onto a flash drive that was inserted into a U.S. military laptop, causing the code to spread rapidly throughout U.S. Central Command’s network and transfer classified information to servers under foreign control. Earlier this year, Google was the victim of cyber theft due to attacks emanating from China. While these and other attacks resulted in limited damage, cyber threats are growing more sophisticated, stealthy, and menacing.

A likely target for attack is the electrical grid. The Department of Energy found that the computer networks controlling the U.S. electrical grid have widespread security flaws that cyber attackers could easily manipulate, potentially putting millions of Americans in the dark. Foreign cyber spies have already placed software within the system that could be activated at any time to bring down the grid.

America is at war—a war being fought over the past decade on an electronic battlefield against malicious hackers and foreign governments dedicated to espionage, corporate theft, and asymmetrical warfare.

THE PROBLEM

The Wild, Wild Web: Cyber war lacks international standards

The pervasiveness of computer networks and advanced information technology in all aspects of modern life has transformed our economy and revolutionized the capabilities of our military and intelligence forces. But it also has made our infrastructure more susceptible to cyber attacks. President Obama calls cybersecurity “one of the most serious economic and national security challenges we face as a nation.” Yet, there are few rules in this new global domain about the responsibilities of nations to prevent and respond to cyber attacks within their borders.

Mutually assured destruction doesn’t work in cyberspace.

During the Cold War, the threat of mutually assured destruction provided the deterrent against superpowers possessing burgeoning arsenals of nuclear weapons. The ability to locate the source of a nuclear attack and retaliate in kind provided a fragile but lasting security equilibrium that withstood periodic flash points between the Soviet Union and the U.S and its allies. Such a security paradigm doesn’t exist with the threat of cyber attack. Attributes who is
responsible for a cyber attack, where they are located, and on behalf of whom they are operating is difficult (if possible) and time-consuming. Options for how to respond and hold attackers responsible are limited as well.

A real world example is the recent “Stuxnet” attack, in which a computer worm that does damage to industrial systems was released. Thought to be the first cyber “guided missile,” the worm infected global networks for a few months before almost all of its infections were taking place in Iran. Although it is thought to have had the positive impact of delaying and damaging Iran’s nuclear program, this type of attack could easily been launched against the U.S.—and it will be almost impossible to determine where it originated.

**Current legislative proposals focus on defense, not on limiting cyber war.**

Members of Congress have introduced several bills to address the growing cyber threat, most of which focus on enhancing U.S. defensive capabilities. While shoring up vulnerabilities to attack is a critical part of cybersecurity, these legislative proposals do not press for the kind of international coordination needed to limit the threat of cyber war. One bill, the International Cyberspace and Cybersecurity Coordination Act of 2010 (S. 3193), addresses part of this challenge by tasking the State Department with providing strategic direction for international cybersecurity policy.

**Unless we act, the cyber threat gap will widen.**

While the U.S. spends billions annually to improve its public and private defenses against increasingly sophisticated and aggressive foreign cyber threats, these advancements alone are not sufficient to lower the risk of a debilitating cyber attack on America’s electrical grid, financial sector or military. Our reliance on networked computer systems will only increase with time as other countries advance their own offensive cyber capabilities and work to mask their detection. As a result, the cyber threat gap will widen unless the international community can come to an agreement on legitimate uses of force in cyberspace, ways of cooperating to determine the sources of illicit cyber activities, and assured methods of responding to cyber attacks.

An international agreement on cybersecurity is the missing piece in the strategy to lower this growing threat and restore deterrence against attack.

**OUR RECOMMENDATION**

**The U.S. should lead with a cybersecurity summit**

The U.S. can demonstrate global leadership by seeking an international accord which would help deter cyber war and, in the process, strengthen our
security and ability to locate and punish cyber attackers. A cybersecurity summit would also ensure that the U.S. is at the forefront of international policymaking in this area and is not hindered by agreements made without U.S. consent. Modeled after the highly successful Nuclear Security Summit held in April, a cybersecurity summit could lay the foundational framework for an international accord which could help prevent cyber war by:

• Improving cooperation among countries to respond to international cyber threats (coordinating counter attacks, helping to block attacks, and sharing information to improve defenses).

• Delineating what are acceptable and legitimate defensive and offensive measures.

• Agreeing on acceptable verification regimes to determine where attacks originate and ensuring that countries of origin take responsibility for attacks initiated within their borders.

• Standardizing and improving cyber defense frameworks in order to protect critical infrastructure.

The summit will build on the growing consensus about the threat and the need for international action.

In a recent speech, the director of the newly formed U.S. Cyber Command, General Keith Alexander, said that “We must leverage all tools of national power to ensure that America and other nations can gain the benefits of free movement in cyberspace and continue to conduct international engagement and diplomacy efforts to improve global governments of this domain.”¹² General Alexander also noted, responding to a recent Russian proposal for a cyber arms control treaty, that “I do think that we have to establish the rules and I think what Russia’s put forward is, perhaps, the starting point for international debate.”¹³

The United Nations, a likely forum for a future international cyber treaty, has also taken steps toward an international accord. In July, 15 countries (including the U.S., China, and Russia) agreed to a set of recommendations aimed at improving international cooperation around cybersecurity, including more discussions about the use of offensive cyber capabilities in warfare.¹⁴

The summit is just the beginning of a potential cyber accord.

The cybersecurity summit would not end with a final agreement on the future of cyber war. Much like the Nuclear Security Summit, though, the goal of the cybersecurity summit would be to end with concrete commitments from its participants on the roadmap ahead. Pre-summit working groups would define the areas of agreement and contention and develop an agenda to move toward
an accord. The areas of agreement would form the basis for a final statement that all participants could sign. The areas of contention would form a “needs agenda” that the participant countries would agree to work on in the future. To be most effective, the final statement out of the summit should include a deadline for producing a final international cyber accord.

**Now is the time to work on preventing cyber war—before a major attack occurs.**

There is common purpose in the global community for reducing the threat of cyber war given the connectivity of information systems and interdependent nature of global economies. The U.S. government and private sector should continue to build strong defensive cyber capabilities as our enemies seek to exploit vulnerabilities. Yet, defensive protections alone will not suffice.

U.S. Deputy Secretary of Defense William J. Lynn III recently wrote that more than 100 foreign intelligence organizations are trying to hack into our military’s digital operational networks. He noted that U.S. military and civilian computer networks are probed thousands of times and scanned millions of times each day. These cyber “velociraptors” are continually testing our defenses for weaknesses. Given the evolving and persistent nature of this threat, an international agreement is needed to establish responsibility, accountability, and deterrence in the shadowy and increasingly dangerous frontier of digital warfare.

* * *

### THE AUTHORS

Andy Johnson is the Director of the Third Way National Security Program and can be reached at ajohnson@thirdway.org. Kyle Spector is a Policy Advisor for National Security at Third Way and can be reached at kspector@thirdway.org. Third Way intern Kristina Lilac provided research and writing assistance for this idea brief.

### ABOUT THIRD WAY

Third Way is the leading think tank of the moderate wing of the progressive movement. We work with elected officials, candidates, and advocates to develop and advance the next generation of moderate policy ideas.

For more information about Third Way please visit www.thirdway.org.
ENDNOTES


3 Ibid.

4 Lynn.

5 Ibid.


10 Legislation introduced in the 111th Congress to improve cybersecurity includes: The Cybersecurity Enhancement Act (H.R. 4061), The Executive Cyberspace Authorities Act of 2010 (H.R. 5247), The Protecting Cyberspace as a National Asset Act of 2010 (S. 3480, H.R. 5548), and The Rockefeller-Snowe Cybersecurity Act (S. 773). While some of these bills include mandates for international cooperation, none have the specific intent of moving toward prevention of cyber war through international cooperation.


15 Lynn.